# الأمن المعلوماتي

## النظام القانوني للحماية المعلوماتية

**Système judiciaire Pour La Protection de L'informatique**




دكتور
طارق إبراهيم الدسوقى عطية



دار الجامعة الجديدة

# الأمن المعلوماتي

# الأمــن المعلوماتى

## «النظام القانونى لحماية المعلوماتى»

## Système Judiciaire Pour

## La Protection de L'informatique

دكتور

**طارق إبراهيم الدسوقي عطيه**

٢٠٠٩م

دار الجامعة الجديدة للنشر 

٣٨ شارع سوتير - الأزاريطة - الاسكندرية ت : ٤٨٦٨٠٩٩

*E-mall.: darelgamaaelgadida@hotmall.com*

بسم الله الرحمن الرحيم

﴿ سَنُرِيهِمْ آيَاتِنَا فِي الآفَاقِ وَفِي أَنفُسِهِمْ حَتَّىٰ يَتَبَيَّنَ لَهُمْ أَنَّهُ الْحَقُّ أَوَلَمْ
يَكْفِ بِرَبِّكَ أَنَّهُ عَلَىٰ كُلِّ شَيْءٍ شَهِيدٌ (٥٣) ﴾

صدق الله العظيم

سورة فصلت

# أهــداء

- إلي روح والدي (الطاهرة) ، نفعني الله جل وعلا بعلمك، وأدخلك برحمته مدخل صدق عند مليك مقتدر.
- إلي أمى الحبيبة.. منبع الحنان.
- إلى زوجتى وأبنائى، منال الحياة ، وقرة العين.
- إلى أستاذى العالم الجليل الدكتور/ هلالى عبد اللاه أحمد.

**مقـدمة:**

مع غـروب شـمس الألفـية الثـانيـة، ودخـول المجتـمع الإنساني ألفـيـة ثالثـة جديدة يتطلع فيها الجميع لمزيد من الحضارة والتقدم والرقى، ومع الانطلاق لآفاق بلا حدود تحمل للبشرية المزيد من الرفاهية والتطور، نجد أنه من الطبيعى فى هذه المسيـرة أن يظهـر تبـاين واضح سـواء فى أنماط التـفكيـر أو فى أنواع السلوك، وبصورة لم تكن مألوفة من ذى قبل بل نقول ويصدق أن هذا التباين لم تتطرق إليه الأذهان مسبقاً أو تتخيله العقول فى السنى الماضية.

ولا تثـريب فى هذا الاخـتـلاف، بل أنـه من الطبـيـعى - والمنطقى - أن نصادفه لأنه سمة الحياة، نلمسه فى منـهج التفكير الذى هو مناط العقل، ونشعر به فى مظاهر الحيـاة ونهـجاً من وقت لآخر، ومن مكان لآخـر رغم التـعاصـر الزمنى. ورغم ذلك يبقى للناس عامل مشترك تجتمع عليه حياة البشر فى كافه ارجاء المعمورة، يحتم وجوده صدق قول الله - تعالى - بشأنه، حيث يعبر عن المصير المشترك للإنسانية ذات الأصل الواحد، حيث يقول تعالى: (يَآ أَيُّهَا النَّاسُ إِنَّا خَلَقْنَاكُم مِّن ذَكَرٍ وَأُنثَىٰ وَجَعَلْنَاكُمْ شُعُوباً وَقَبَآئِلَ لِتَعَارَفُوآْ)(١).

ومن الأمور التى يتضح فيها ملامح التباين بشكل واضح السلوك الإنسانى (Behaviour human)(*)، الذى يصدر عن الإنسان كله باعتبـاره وحدة نفسية جسمية متفاعلة متكاملة يعيش فى بيئة مادية اجتماعية، وهو نشاط يشمل الكائن

---

(١) سورة الحجرات - الآية: ١٣.

(*) للمزيد بشأن السلوك الإنسانى يراجع مؤلفنا المعنون: الشخصية الإنسانية (بين الحقيقة وعلم النفس)، دار الجامعة الجديدة - الإسكندرية - سنة ٢٠٠٧ - ص ١٠٦ وما بعدها.

* ويقصد بالسلوك جميع الأنشطة التى يقوم بها الكائن الحى، وبذلك يدخل تحت مفهوم السلوك المناشط العقلية والفسيولوجية التى تحدث داخل الكائن الحى ذاته، ولا يقتصر السلوك الإنسانى على أوجه النشاط الظاهر (كالكلام والمشى والحركة)، وانما يتعداه إلى السلوك الضمنى (الذاتى) الذى يتمثل فى التفكير والتخيل والتذكر والانفعال....

إن السلوك الإنسانى هو كل أوجه نشاط الفرد الذى يمكن ملاحظته سواء بالادوات القياسية أو بدونها. (د/ طارق ابراهيم الدسوقى - المرجع السابق - ص ١٠٧).

كله ويقوم به الإنسان برمته، ويحمل السلوك الإنسانى الكثير من المكونات والمتغييرات والتطورات التى يصعب فهمها وفى بعض الأحيان تفسير أبعادها، وكان هذا الأمر موضع اهتمام ودراسة الكثير من العلماء والمختصين فى جانب من أفرع العلوم الاجتماعية مثل علم النفس وعلم الاجتماع وما يتصل بهما من فروع.

والسلوك الإنسانى فى جانب منه سوى، كما وأنه فى جانب آخر غير سوى (شاذ) يصطدم بأنظمه الحياة الطبيعية التى يحياها الكثير من الناس، تحمل هذه الحياة مظاهر الخير ولا تخلو من بعض مظاهر الشر، الذى نلمسه بشكله البغيض ولونه القاتم يتمثل فى سلوك إجرامى لا يخلو منه المجتمع، أنه صراع الحياة بين الخير والشر القائم والمستمر منذ بدء الخليقة وعلى مر الأزمنة الغابرة والحاضرة والقادمة.

وكلما تقدمت البشرية واخذت سبيلها للرقى والنهوض، تبعها الجانب المظلم فى النفس البشرية بتقديم أصناف مطورة من الجرائم غير المألوفة، أنها المحصلة الطبيعية والمنطقة لتطور الحياة البشرية ورقى المجتمعات، فلم تعد الجريمة من ذات التوصيف القانونى المألوف سرقة أو اختلاس أو نصب بذات المفهوم التقليدى، ولكنها تطورت مع تطور النظام القانونى العالمى أو الإقليمى. فاستهدفت جريمة السرقة بطاقات الائتمان والشبكات السياحية، وتعدت جريمة الاختلاس نطاقها الاقليمى ليكون من السهل ان تمتد عمليات الاختلاس لبنوك فى بقعه أخرى ودولة ثانية، كما تحولت جريمة النصب إلى تعدد النطاق المكانى بين الدول لتشمل عند ارتكابها أكثر من دولة. والقاسم المشترك فى هذا السلوك الإجرامى هو ما ورثه العالم من تكنولوچيا حديثة، وتقنية معلوماتية عالية المستوى.

إنها المحصلة النهائية للتطور العلمى للمجتمع، ولكن نؤكد بأنه دائماً (الجريمة لا تفيد)، وقد يجنى مقترفها بعض المزايا المؤقتة الزائفة، ولكن

سرعان ما ينتهى ذلك وتعود الأمور إلى نصابها الصحيح، لأن ثورة العلم من أجل خير البشرية، ومن يحيد عن هذا الهدف، فإن المجتمع يملك من الآدوات والمزايات الكفيل والكافى لردع المارق عن الشرعية والمنتهك للنظام.

لقد أفرز التطور العلمى والتكنولوچى الذى يعد أحد مظاهر العصر الحديث، ثورة فى الاتصالات والمعلومات(*)، باتت تلك الأنظمة والعناصر المكونهة لها فى حراك تقنى متزايد ليس يوماً بعد يوماً، بل تعدى تطور التقدم فى الاتصالات والمعلوماتية الاجزاء الزمنية الصغيرة... ويعد من الوسائل المستحدثة فى أنظمة ثورة الاتصالات والمعلومات ما يطلق عليه (الحاسب الآلى)، والذى يعد بلا شك من أهم وسائل هذه الثورة، نظراً لتعدد وظائفه وزيادة قدرته العملية والإنتاجية، وتعقيد مكوناته واجزائه. إن العالم يعيش فى هذه الأونة وبحق عصر المعلومات، ومن يدرى ما هى اختراعات العلم فى المرحلة المقبلة.

- **العصر المعلوماتي:**

يشهد العالم اليوم عصراً جديدا يطلق عليه المفكر الأمريكى ألفين توفلر(**)

(*) يقصد بثورة الإتصالات والمعلومات تلك النقلة الحضارية المتطورة فى وسائل الاتصال، التى تعددت وتنوعت وأضحت أكثر كفاءة عن ذى قبل، فالمتتبع لأنظمة الاتصالات السلكية واللاسلكية مثل الهاتف والبرق والبريد والفاكس، ثم المرحلة التالية وهى نقل الأنباء بالصوت فقط، ثم بالصوت والصورة معاً وهو ما تمثل إجمالاً فى المذياع (الراديو) وشبكات التلفاز سواء الإقليمية أو العالمية، ثم الفضائيات التى أنتشرت فى انحاء الكون، وغطت أخبار العالم بأسره بامكانيات علمية مذهلة، نقلاً للاحداث وقت حدوثها، ثم النقلة المعلوماتية الأهم على المستوى الوطنى والدولى، تلك المعروفة بـ (شبكة الأنترنت) التى يمكن من خلالها استعراض المعلومات والبيانات وذلك من خلال شبكة تغطى العالم (World Wide Web) والتى يطلق عليها اختصاراً (www)، الأمر الذى غدا معه العالم أشبه بقرية كونية صغيرة، يؤثر ويتأثر سكانها بما يقع من احداث فى أى من أجزائها، وهذا ما أطلق العنان لمفهوم العولمة (Globalization) أن ينطلق بالنظر إلى عالمية النتائج المترتبة عن ما يقع من احداث على مستوى العالم.

(**) المفكر الأمريكى: ألفين توفلر هو أحد رواد علم المستقبل Futurology فى العصر الحديث، ويقصد به ذلك العلم الذى يحاول استنزاف السنوات القائمة فى دولة معينة أو مجموعة من

=/=

(Alven Tovilr) العصر المعلوماتي أو عصر ثورة المعلومات(*)، وقد نشأت هذه الثورة من جماع طفرتين هما: طفرة الاتصالات وطفرة تقنية المعلومات، فلقد حدثت طفرة فى الاتصالات حولت العالم إلى قرية صغيرة، وربطت بين الشعوب المتباعدة، فأصبح الإنسان يستطيع أن يرصد ما يجرى على الطرف الأخر من الكرة الأرضية بالصوت والصورة فى لحظة قيام الحدث، وأصبحت عملية تبادل المعلومات والمعارف سهلة ميسورة، وأدى انتشار المعلومات السريع عبر وسائل الاتصال المختلفة إلى تدفق هائل فى المعلومات والأخبار والمعارف والأبحاث والرسائل الثقافية(**)، يعجز الإنسان بقدرته العادية عن متابعتها والإلمام بها فى عمره القصير(١).

كذلك حدثت طفرة فى تقنية المعلومات تمثلت فى اختراع وتطوير الحاسب الآلى الذى أضاف للإنسان قدرات هائلة على الاحتفاظ بالمعلومات ومعالجتها بسرعة خيالية لم تكون تخطر على بال الإنسان من قبل، فقد أصبح من المعروف الأن أن عقل الحاسب الآلى يستطيع أن ينجز فى ساعة من الزمن ما لا يستطيع عدد من العلماء إنجازه فى سنة عمل متواصل، وهكذا نشأ عن اجتماع تكنولوچيا الاتصالات وتكنولوجيا الحاسب الآلى ثورة حقيقة فى

---

— الدول استشراقاً علمياً منهجياً من أجل تطويرها على الصورة المبتغاة أو المأمولة. ولمزيد من المعلومات يراجع: الفين توفلر (الموجة الثالثة) ترجمة فادى غصون – دار الروح – (بيروت) لبنان – سنة ١٩٨٥، وأيضاً: آلفين توفلر (وعود المستقبل) ترجمة فادى غصون – دار الروح – (بيروت) لبنان – سنة ١٩٨٩.

(*) ولذا أصبحت صناعة المعلومات مصدراً للثروة ومقياساً لتقدم الأمم بل وأساساً للقوة الاقتصادية والسياسية والعسكرية.

(**) فلقد تسارع معدل نمو العلم بصورة مذهلة لم يسبق لها مثيل فى أى عصر من العصور المنصرمة، إذ تقول الإحصاءات أن كمية المعرفة البشرية تتضاعف حالياً خلال فترة تتراوح بين خمس إلى عشر سنوات، وهو ما كان يستغرق فى ماضية سنوات.

(١) د/ هلالى عبد اللاه أحمد – حجية المخرجات الكمبيوترية فى المواد الجنائية – دار النهضة العربية – سنة ١٩٨٨، ص ٥.

المعلومات، حيث أدت ثورة الاتصالات إلى تراكم مذهل في المعرفة وحصيلة هائلة فى المعلومات تعجز الوسائل البشرية عن ملاحقتها وفهرستها، واستخلاصها وتصنيفها ومعالجتها والاستفادة منها والسيطرة على تدفقها من مصادر متباينة ومتنوعة، فجاءت تكنولوجيا الحاسب الآلى لتقدم خدمة جليلة للإنسان بما يمكن هذا الاختراع الثورى من دقة وسرعة فى جمع المعلومات وتحليها ومعالجتها وتوزيعها واسترجاعها فى وقت يسير(١).

ومع هذا التطور المعلوماتى الهائل، فإن هناك سمة بارزة فى تكنولوجيا المعلومات تتمثل فى الأثر الذى احدثته ومازالت تحدثه على تطور تكنولوجيا الاتصالات عن بعد،فالتليفون التقليدى الذى كان يقتصر على تبادل الصوت البشرى، قد أصبح الآن يتبادل كميات هائلة من البيانات التى يمكن أن تحتوى على أصوات ونصوص وأنغام موسيقية وصور فوتوغرافية وأفلام سينمائية، وهذا التبادل لم يعد يحدث فقط بين البشر، ولكنه أصبح يحدث أيضاً بين البشر وأجهزة الحاسب، بل وبين أجهزة الحاسب بعضها البعض، كذلك يكفى أن يتم إدخال البيانات إلى شبكة معينة من خلال عنوان المرسل إليه حتى تصبح متوافرة لإى شخص يريد الدخول إليها(*).

---

(١) المرجع السابق، ص ٦.

وللمزيد يراجع: آلان بونيه: (الذكاء الاصطناعى واقعة ومستقبلة)، ترجمة د/ على صبرى فرغلى – سلسلة عالم المعرفة – الكويت – أبريل سنة ١٩٩٣، ص ٢٣٥ وما بعدها، د/ محمد فهمى طلبة وآخرون – الحاسب والذكاء الاصطناعى – موسوعة دلتا كمبيوتر ١٠ – القاهرة – مطابع المكتب المصرى الحديث – سنة ١٩٩٤ – ص ٣٠٣ وما بعدها.

(*) المذكرة التفسيرية لاتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١ بشأن الإجرام المعلوماتى أو الجرائم المعلوماتية

(Convention sur la cyber Criminalité, Budapest 32, x.I. 2001).

د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١) – القاهرة – دار النهضة العربية – الطبعة الأولى – سنة ٢٠٠٣، ص ٣٠.

كما أن الاستخدام العام للبريد الالكتروني Le Courrier êlectronique، ووصل الجمهور لمواقع الويب Sites Web(*) عبر الانترنت من أمثلة هذا التطور الذى قلب أوضاع مجتمعنا، كذلك فأن سهولة الوصول إلى المعلومات فى النظم المعلوماتية، مع الإمكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المسافات الجغرافية أدى إلى نمو هائل فى حجم المعلومات المتاحة، والتى يمكن الحصول عليها، ومن خلال الاتصالات بخدمات الاتصالات والمعلومات يستطيع المستخدمون Les Usagers اصطناع فضاء جديد يسمى الفضاء المعلوماتى Srber espace(**)، الذى يستعمل – أساساً – لأغراض شرعية، ولكن يمكن أن يخضع لسوء الاستخدام، إذ هناك احتمال لاستخدام شبكات الحاسب والمعلومات الاليكترونية فى ارتكاب أعمال إجرامية، وعلى ذلك يجب على القانون الجنائى أن يحافظ على مواكبته لهذه التطورات التكنولوجية، التى تقدم فرصاً واسعة

---

(*) يقابل ذلك فى المصطلح الانجليزى لاتفاقية بودابست ٢٣ نوفمبر ٢٠٠١ Web Sites، وهو يعنى مجموعة وثائق مترابطة تمثل وحدة من وحدات www مخدومة بخادم Http، وكلمة Web تعد اختصاراً لعبارة World Wide Web بمعنى الشبكة العنكبوتية، وهى عبارة عن خدمة إعلامية واسعة النطاق على المستوى العالمى، نشأت على يد CERN فى بداية التسعينات، تضم وثائق متشعبة Hypertexts مدعمة بنظام الميديا أى الوسائط المتعددة والمتشبعة Hypermedia مخزنة على خادمات البروتوكول Http متصلة بشبكة الانترنت، وتسمى هذه الوثائق صفحات الويب Web Pages وتصاغ بكلمة HTML ويمكن الوصول لمواقع هذه الخدمة عن طريق مميز المصادر URC.

ـ وبالنسبة لكلمة Http فانها تعد اختصار لعبارة Hypertext Transfer Protocol أى بروتوكول نقل النصوص المتشعبة بين الحاسبات، وبالنسبة لكلمة HTMl فأنها اختصاراً لعبارة Hyper-text mark up Languge أى لغة اتش تى أم إلا وهى لغة تعبئة تستخدم لتصميم صفحات الويب. د/ هلالى عبد اللاه أحمد – المرجع السابق – هامش ص ٣١.

(**) يقابل ذلك فى المصطلح الانجليزى Cyber - Space بمعنى الفضاء المعلوماتى، وهو عبارة عن كم الإمكانيات المتاحة عن طريق الانترنت وغير ذلك لتبادل المعلومات عن نطاق كونى. وقد استخدم اللفظ الاجنبى لأول مرة فى راوية للمؤلف الروائى وليام جيبسون Willim Gib-son فى رواية Neuro Mancer عام ١٩٨٢. (راجع على يوسف على – معجم مصطلحات الحاسب – القاهرة – دار خوارزم – ص ١٧٨).

لإساءة استخدام إمكانيات الفضاء المعلوماتى وأن يعمل على ردع هذه الأفعال الإجرامية، مع تطبيق السلطات القسرية المقررة فى بيئة تكنولوجيا المعلومات(١) .

وإذا كان العصر المعلوماتى Informaticc Age أو عصر ثورة المعلومات In-formation Revolutaion هو نتاج طفرة الاتصالات Communications، وطفرة تقنية المعلوماتInformation Technical، فإن ما جاء به من أنشطة غير مشروعة تنطوى – بلاشك – على أنشطة إجرامية تقليدية تأخذ شكلاً مستحدثاً(٢) .

**• مدي أهمية العصر المعلوماتي دولياً وإقليمياً:**

فى نهاية القرن العشرين وبداية القرن الحادى والعشرين تعرض العالم بأسره إلي مشكلة كانت بحق هى أزمة القرن العشرين، دفعت جميع المستويات الدولية للوقوف مجتمعه لمواجهتها. كما دفعت هذه الأزمة رأى فى الفقه(٣) إلى استرجاع تساؤل شهير للكتاب القرنسى الشهير موليير Moliere (*) قاله منذ ما نييف على ثلاثة قرون في مسرحية(**) (آلاعيب سكابان Les fourrberies de Scapicn):

---

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٣٢.

– ولهذا الشأن تم صياغة المذكرة التفسيرية لإتفاقية بواديست الموقعة فى ٢٣ نوفمبر ٢٠٠١ . وتتكون هذه الإتفاقية من ثمانى وأربعين مادة موزعة على أربعة أبواب كما يلى: «يعالج الباب الأول استخدام المصطلحات Terminologie ويتناول الباب الثانى الإجراءات الواجب اتخاذها على المستوى القومى. والباب الثالث تم تخصيصه لدراسة التعاون الدولى Coopération intenationale والباب الرابع يتعرض للشروط الختامية Clauses Einales .

(٢) محمد أمين أحمد الشوابكة – جرائم الحاسوب والانترنت (الجريمة المعلوماتية) – عمان – مكتبة دار الثقافة للنشر والتوزيع – الطبعة الأولى – سنة ٢٠٠٤ – ص ٧.

(٣) د/ هلالى عبد اللاه أحمد – قانون العقوبات وأزمة الحاسبات – دار النهضة العربية – سنة ١٩٩٨ – ص ٧ وما بعدها.

(*) ولد موليير فى عام ١٦٢٢ وتوفى عام ١٩٧٣ عن عمر يناهز الواحد والخمسين عاماً. ويعد أحد أعظم كتاب المسرح والكوميديين فى جميع العصور – راجع فى ذلك: «منير البعلبكى: (المورد قاموس إنجليزى – عربى) بيروت – دار العلم للملايين – ط ٣٢، معجم أعلام Biographical Names -- سنة ١٩٩٨ – ص ٦١.

(**) موليير (ألاعيب سكابان)، الفصل الثانى، المشهد الحادى عشر.

"Moliere": "Les Fourberies de Scapin: Acte 2, Scéne xI.

ماذا كان سيفعل الشيطان فى هذا القارب؟ Que diable allait - il Faire dans cette galére? وقد أضاف الرأى الفقهى لهذا السؤال، وماذا سنفعل نحن في مواجهة هذا الشيطان، بعد أن بات العالم بأسره على متن هذا القارب؟ ماذا أعددنا لمواجهة شيطان القرن الحادى والعشرين؟ أو مشكلة عام ٢٠٠٠ The Year 2000 Problem،(١).

أو مشكلة....Y2k (*)، أو مشكلة الحاسبات الآلية عام ٢٠٠٠ Year 2000

---

(١) ومن أمثلة البحوث والتقارير التى تحمل هذا العنوان نذكر على سبيل المثال:

-BALL. (Keyser Mason): "The Year 2000 Problem: Get That Finger off The Snooze Buton!", Mississauge, ONTARIO. CANADE., 1997.

- DELANCY (Benjamin J.): "The Year 2000 Problem: Paying The Programmers" San Francisco office. Thelen, 1997.

- GRABBE (J. Orlin): "The Year 2000 Problem in Perspective" December 28, 1997, U.S.A.

- KAPPELMAN (Leon A.) and CAPPEL. (James J.): "Critical issue report Facing The Year 2000 Problem" College of Business Administration University of North Texas, U.S.A. Aprit 1996.

(*) يشير الحرف الحادى عشر فى الأبجدية الفرنسية K إلى رمز كيلو Kilo وتعنى ألف وحدة سواء كانت وحدة وزن أو قياس أو إحصاء. فنقول كليو جرام Kilogramme (K.G.) أى وحدة وزن تساوى ألف جرام وكيلو متر Kilométre (K.M.) أى وحدة قياس تساوى ألف متر، وكيلو طن Kilotonne (K.T.) أى ألف طن، وكيلو وات Kilowatt (K.W.) أى وحدة لقياس الطاقة تساوى ألف وات. وفى مجال قياس سعة ذاكرة الحاسبات الآلية نقول كيلو بايت (K.B.) Kilo Byte أى ألف حرف. وعلى ذلك إذا قلنا Y2K فمعنى ذلك إننا نشير إلى مشكلة عام ٢٠٠٠. راجع فى وحدات الوزن والقياس.

* د/ سهيل إدريس: «المنهل قاموس فرنسى عربى» – بيروت – دار الأداب – الطبعة التاسعة عشرة – سنة ١٩٩٨.

* د/ محمد فهمى طلبة وآخرون: «الموسوعة الشاملة لمصطلحات الحاسب الألكترونى» – مرجع سابق – ص ٢٥٧.

* ومن أمثلة التقارير والبحوث التى تحمل عنوان Y2K نذكر:

عنوان الكلمة التى ألقاها رئيس المؤتمر الذى أقامته الأمم المتحدة فى نيويورك بحضور ٢٠٠ خبير يمثلون ١٢٠ دولة لمناقشة مشكلة عام ٢٠٠٠ وخطط الطوارئ اللازمة لمواجهتها وذلك فى يوم الجمعة الموافق ١١/١٢/١٩٩٨:

=/=

أو.(**) The Year 2000 Crisis أو أزمة عام ٢٠٠٠ .(*) Computer Problem

---

- "National Y2k Coordinators meeting" The United Nations, December II, 1998. New York, Meeting The Global Challenge Chairman's Summary of Meeting.
- ISHAK (Bahget M.A.): "Views on Y2k Application Testing" - Extracts from Stephen J. Gerrad's Paper on Aplan for Year 2000 Testing", Assiut University Network Center, Management of The Year 2000 Crisis, Symposium Proceedings, Assiut 29, 30 September 1998, p. 11.
- GOODSPEED (Peter): "Hi - Tech experts race to Zap Y 2 Bug", Canada. Toronto Star Feature Writer, August 23, 1998.

(*) ومن أمثلة المقالات والبحوث والمؤتمرات التى تحمل هذا العنوان راجع على سبيل المثال:

- GAHTAN (Alan) - MANN (J. Fraser): "Year 2000 Computer Problems", February 19-20, 1998, Metropolitan Hotel, TORONTO, CANADA - "Year 2000 Legal Conference.
- KAPPELMAN (Leon A.), JOHNSON (Jerry I.) and ROSMOND (Kathy): "The Role if government in Solving The Year Computer Problem", In Year 2000 Problem: Strategies and Solutions from The Fortune 100", International Thomson Computer Press U.S.A. 1997.
- "Year 2000 Computer Problems managins risk and Legal issues" Conferences - June 22-23, 1998, Holiday Inn Calgary Downtown, Calgary, Canada.
- "Information about Year 2000 Computer Problem", Australian in formations industry Association, 20 April 1998, (AIIA).

(**) كانت هذه الصيغة عنواناً لندوة إدارة أزمة الحاسبات عام ٢٠٠٠ التى أقامها مركز شبكة معلومات جامعة أسيوط فى الفترة من ٢٩ – ٣٠ سبتمبر بأسيوط – سنة ١٩٩٨.

- "Management of The Year 2000 Crisis Symposium Proceedings", assiut University Network Centre, 29-30 september 1998.

وراجع أيضا:

- "The Need for Immediate Action at The Highest Corporate Levels to Solve The Year 2000 Soft ware Crisis" U.S.A. Comlinks, 1997.
- http: // WWW. Comlinks. Com / Legal / Tmjb2.htm.

أزمة كمبيوتر عام ٢٠٠٠ The Year 2000 Computing(*). أو الأزمة العالمية لعام ٢٠٠٠ A World Wide Year 2000 Crisis. أو تحدى عام ٢٠٠٠ The Year 2000 Challenge(**). أو عبء أو تكلفة عام ٢٠٠٠ Down load 2000 (1). أو مشكلة التحول لعام ٢٠٠٠ Year 2000 Conversion(***).

---

(*) وقد كانت هذه الصياغة عنواناً لتقرير أصدره مكتب المحاسبة العام بالولايات المتحدة: «أزمة كمبيوتر عام ٢٠٠٠ دليل للتقويم يتضمن قائمة اختبار نموذجية عن الأعمال التى يجب القيام بها للتأكد من التوافق مع عام ٢٠٠٠.

- The "Year 2000 Computing Crisis: an Assessment guide" The Unites States General Accounting office.

مشار إليه لدى:

- Anne xD - Recommendations of world in formation technology services Alliance - The Untied Nations: "National Y2K Coordinators meeting December II, 1998 New York, p. 5.

(**) وردت هذه الصيغة ضمن مفردات عنوان المؤتمر الذى أقامته الأمم المتحدة فى نيويورك لمناقشة عام ٢٠٠٠ فى ١١/١٢/١٩٩٨، كما وردت هذه الصيغة بوصفها عنواناً فى التقرير المقدم من قسم خدمات تكنولوجيا المعلومات بالأمم المتحدة.

- "The Year 2000 challenge for the United Nations: A report to the ECOSOC Working group on informaties, Prepared by The information Technology Services Division, November 1997.

(١) ويقابل هذا العنوان بالفرنسية:

- Du Téléchargement, 2000,

(***) وردت هذه الصيغة ضمن عنوان التقرير المقدم من الأمين العام للأمم المتحدة للجمعية العامة فى دورتها الثالثة والخمسين، والذى يتضمن الخطوات التى تم اتخاذها داخل جهاز الأمم المتحدة والدول الأعضاء لحل مشكلة الحاسبات عام ٢٠٠٠، كما وردت أيضاً ضمن عنوان الكلمة التى ألقاها الرئيس الأمريكى (بيل كلينتون) فى الأكاديمية الوطنية للعلوم فى ١٤ يوليو سنة ١٩٩٨.

- "Remarks by the president concerning the Year 2000 conversion:, National Academy of Sciences, U.S.A. July 14. 1998, The White House office, of the Press Secretary.

ويقابل هذا العنوان بالفرنسية:

- Conversion De L'Année, 2000.

وكل هذه النعوت والصفات إنما كانت تعبر عن مدى جسامة النتائج التى كان يمكن أن تحيق بالدول التى توقفت ولم تشرع فى توفيق أوضاعها الكمبيوترية مع منطقية عام ٢٠٠٠، فالمتتبع لواقع هذه الأزمة وتداعياتها تفجعه صورة قائمة كئيبة للآثار المدمرة التى كانت ستصيب كل مناحى الحياة، فى حالة فشل نظم الحاسبات الآلية وما تحتوى من نظم مطورة، عن استمرار التشغيل مع مطلع عام ٢٠٠٠.

أنها مشكلة ذات صبغة تقنية وقف العالم بأسره على اعتابها، محاولاً التغلب عليها والنجاة من أثارها واسعة النطاق، يدفعنا هذا للتأكيد على أهمية المعلوماتية فى عصرنا الحديث على المستوى الدولى والوطنى، وأنه أن كان الجميع قد أدرك مدى خطورة أزمة المعلوماتية مع مطلع الألفية الثالثة، فإن الوضع لا يزال على ذات الخطورة، نتيجة للأنشطة الإجرامية المتزايدة التى تصيب المعلوماتية بعناصرها ونظمها.

- **أشكالية الدراسة:**

- **الحاجة الماسة إلي تشريع جنائي لمواجهة الإجرام المعلوماتي:**

إن الدراسة المتأنية للنظام التشريعى الجنائى فى مصر تبين ضآلة الحماية الجنائية المنبسطة لحماية النظام المعلوماتى. حيث أدى التقدم العلمى والتطور التكنولوجي إلى ظهور الحاسب الآلى، وشاع استخدام المعالجة الآلية للمعلومات فى شتى مجالات الحياة، نظراً لما يتمتع به الحاسب الآلى من قدرة فائقة على تخزين البيانات والمعلومات وترتيبها وتصنيفها على نحو ييسر الحصول عليها بسرعة فائقة(١). كما ذاع استخدام الحاسب الآلى فى المجالات الاقتصادية والعسكرية والسياسية والاجتماعية، وقد أدى تنوع مجالات استخدام الحاسب

---

(١) محمد عقاد – جريمة التزوير فى المحررات للحاسب الآلى (دراسة مقارنة) – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – الفترة من ٢٥:٢٨ أكتوبر ١٩٩٣ – ص ٣.

الآلى إلى تنوع فرص واحتمالات الاعتداء على برامجه وسرقتها وإتلافها وتزويرها واستخدامها بدون وجه حق[1].

وهكذا أصبحت برامج الحاسب الآلى محلاً لانتهاكات مدنية[2]، وجرائم جنائية عديدة على نحو اقتضى توفير أكبر قدر ممكن من الحماية المدنية والجنائية لهذه البرامج، وذلك لمواجهة هذه الظاهرة الإجرامية فى مجال المعلوماتية(*).

---

(١) د/ هدى حامد قشقوش – جرائم الكمبيوتر وجرائم تكنولوجيا المعلومات – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى – المرجع السابق – ص ١.

(٢) محمد محمد شتا – فكرة الحماية الجنائية – لبرامج الحاسب الآلى – دار الجامعة الجديدة – الإسكندرية – سنة ٢٠٠١ – ص ٨.
حيث عرض لقصور الحماية المدنية لبرامج الحاسب الالى.

(*) بدأ الفقه يتعرض فى مجال الإجرام المعلوماتى إلى:
أولاً: موضوعات وثيقة الصلة بقدرات الحاسبات الآلية على تخزين المعلومات واسترجاعها، مثل دراسة الحماية الجنائية للحياة الخاصة والحريات الشخصية وبنوك المعلومات.
مبدر سليمان الويس – أثر التطور التكنولوجى على الحريات الشخصية – كلية الحقوق – جامعة القاهرة – سنة ١٩٨٢ – ص ١٥٢، د/ أسامة عبد الله فايد – الحماية الجنائية للحياة الخاصة وبنوك المعلومات – بدون ناشر – القاهرة – سنة ١٩٨٨ – ص ٢٨.
* ويقصد بتعبير بنوك المعلومات Banques de données: عملية تكوين قاعدة بيانات تفيد موضوعاً معيناً وتستهدف خدمة غرض معين ومعالجته بواسطة أجهزة الحاسب الإلكترونية وأيضا يراجع فى تأثير تطور علم الحاسب الآلى على أسرار الحياة الخاصة.. د/ طارق أحمد فتحى سرور – الحماية الجنائية لاسرار الأفراد فى مواجهة النشر – دار النهضة العربية – سنة ١٩٩١ – ص ١٩٨. مشيراً إلى أنه:
أصبح التوصل إلى البيانات والحقائق عن الأفراد أكثر سهولة من ذى قبل بفضل الحاسب الآلى، وقد أدى ذلك إلى زيادة الحاجة إلى اتخاذ الحيطة اللازمة للمحافظة على أسرار الأفراد، وفى صدر هذه المشكلة توجد مشكلتان فرعيتان:
الأولى: تتعلق بالكمبيوتر كوسيلة تكنولوجية لجمع المعلومات التى تهدد حرمة الحياة الخاصة.
الثانية: تتعلق باستعمال المعلومات المودعة فى الكمبيوتر بما يتضمنه من نشر لأسرار الحياة الخاصة الكامنة فى هذه المعلومات.
ثانياً: موضوعات جرائم الحاسب الآلى والحماية القانونية (المدنية والجنائية) لبرامج الحاسب الآلى.
-/-

وإذا كانت الدول المعنية بحماية نظم المعلوماتية - ورغم أصدارها لتشريعات تجرم انتهاك نظم المعلومات - تجد صعوبة فى كثير من الأحيان، فى بسط النفوذ القانونى وحماية البرامج الحاسوبية والنظم المعلوماتية، بسبب استخدام التكنولوجيا المتقدمة فى أساليب الاعتداء عليها. فان الأمر يحتاج إلى أهتمام أكثر وعناية قانونية أعمق من الدول النامية - ومنها مصر - تحسباً لأنه في الفترة القادمة سوف تتفشى مظاهر الاعتداء على نظم المعلوماتية، وتزداد جرائم المعلوماتية بصورة تعجز الدولة على مجابهتها، ومواجهتها بالقواعد القانونية التقليدية التى صيغت لتجريم نشاط وسلوك إجرامى مختلف ينصب على المنقولات المادية والأفعال التقليدية.

ختاماً.. فإنه بالنسبة للمعلومات ونظمها وسبل معلاجتها آليـاً، فإن الأمر لا ينبغى أن يترك لتفسير الفقة، واجتهاد القضاء، من أجل بسط القواعد القانونية القائمة. ومن الأفضل - أن لم يكن من الأصوب - أن يتناول المشرع المشكلة بالفحص والدراسة والتمحيص، ما أجل سن تشريع خاص - تأسياً بالمشرع الفرنسي - يتناول تجريم الأفعال المتصور أن تصيب المعلوماتية ونظمها وبرامجها. ويبقى أن نذكر أن النصوص القانونية المبتغاه لحماية نظم المعلومات، هى الهدف المنشود الذى تقصده الدراسة، لعلاج القصور التشريعى الحالى فى هذا الصدد.

---

-- ذلك أن هذه البرامج هى جوهر الكيان المعنوى للحاسبات، ومن غيرها لا يكون للحاسب الآلى قيمة سوى أهمية وفاعلية تلك المواد التى يتم تصنيعها منها، فالبرامج هى التى يتحقق من خلالها قيام جهاز الحاسب الآلى بأداء وظائفة المتعددة.

د/ على عبد القادر القهوجى - الحماية الجنائية لبرامج الحاسب الآلى - مجلة الحقوق للبحوث القانونية والاقتصادية - كلية الحقوق - جامعة الإسكندرية - سنة ١٩٩٢ - ص ٢٧١.

مشار إلى ما سبق لدى: محمد محمد شتا - المرجع السابق.

● **الإجراءات المنهجية المتبعة:**

يعتبر أسلوب البحث العلمي من المسلمات في أي مجال من مجالات المعرفة الإنسانية. ولذا بات الإلمام بمنهجية هذا الأسلوب بدء من تحديد المشكلة ومروراً باختيار منهج أو طريقة جمع المعلومات وانتهاء بتحليل هذه المعلومات واستخلاص النتائج منها، من الأمور الضرورية التي يتعين على كل باحث مراعاتها، والتقيد بها(*).

والملاحظ أن طبيعة المشكلة محل الدراسة، تلعب دوراً رئيسياً في اختيار وتحديد المنهج الذي سيتم اتباعه، ومن هذا المنطلق فأنه سوف نستعين في بحثنا بمجموعة من مناهج البحث، فالإضافة لاستخدام المنهج الوصفي التحليلي، لتوصيف مظاهر أمن المعلوماتية، ونوعية الجرائم التي تصيبها، وتحليل كل فعل يشكل جريمة، وتحديد الفئات التي تقوم بهذه الأفعال، تم الاستعانة بالمنهج التأصيلي التطبيقي لاستعراض الآراء النظرية والفقهية بشأن تقسيم الجرائم المعلوماتية، ونظراً لحداثة تلك الجرائم بالنسبة للفقه والقضاء المصري، فإنه كان من الضروري استخدام المنهج المقارن لعرض التشريعات القانونية المختلفة التي نظمت ذات الموضوع. وختاماً تم تسطير إستراتيجية متكاملة لتوفير سبل الأمن المعلوماتي من خلال الاستعانته بالمنهج الوصفي التكاملي.

**وبعد فهذا اجتهاد، قمت به قاصداً الخير والعلم والمعرفة، هو خالصاً لوجه الله (تعالي)، فإن وفقت فيه فذلك من فضل الله، وإن قصرت فذلك من سمات البشر، وحسبي المحاولة والاجتهاد.**

**الإسكندرية شتاء ٢٠٠٨** **طارق الدسوقي**

---

(*) والمنهج في اللغة: النهج هو الطريق المستقيم الواضح، والمناهج هي الخطة المرسومة، والمنهج الطريق المبين إلى الحق في أيسر سبله. (المعجم الوسيط – جـ٢ – ص ٩٦٦).
واصطلاحاً: المنهج الطريق المؤدى إلى كشف الحقيقة في العلوم، بواسطة طائفة من القواعد العامة تهيمن على سير العقل وتحدد عملياته، حتى يصل إلى نتيجة معلومة.

فصل تمهيدي

# الأمن والمعلوماتية

## (ماهية الأمن - وماهية المعلوماتية)

- المبحث الأول: ماهية الأمن.

    المطلب الأول: مفهوم الأمن.

    المطلب الثاني: من تعريفات الأمن.

- المبحث الثاني: ماهية المطوماتية.

    المطلب الأول: تعريف المعلوماتية.

    المطلب الثاني: عناصر المعلوماتية.

# المبحث الأول

# ماهيــــة الأمــن

الأمن من الضروريات الرئيسية لوجود المجتمع واستمراره، ولا أدل على ذلك من قوله تعالى في كتابه الكريم: (لِإِيلَافِ قُرَيْشٍ إِيلَافِهِمْ رِحْلَةَ الشِّتَاءِ وَالصَّيْفِ، فَلْيَعْبُدُوا رَبَّ هَذَا الْبَيْتِ الَّذِي أَطْعَمَهُم مِّن جُوعٍ وَآمَنَهُم مِّنْ خَوْفٍ)(1).

فحاجة الإنسان للأمن تعادل حاجته للطعام والشراب والمسكن وهو أهم ما يلزم لبناء حياته، وقد حث الله سبحانه وتعالى على الأمن لأنه نعمة على عباده، والأمن لا يلتقى مع القلق والاضطراب، بل أن الأمن شرط لتحقيق الاستقرار والحياة الهادئة، وهو مظهر لسيادة القانون والنظام.

ولم يكن مفهوم الأمن في الإسلام مقتصراً على طيبات الحياة الدنيا، إنما تجاوزها إلى حاجات النفس، فالأمن كما نفهمه في عقيدتنا السمحاء غذاء للروح والقلب، وقد تضمن القرآن الكريم آيات تحمل هذا المعنى العميق قال تعالى: (الَّذِينَ آمَنُوا وَلَمْ يَلْبِسُوا إِيمَانَهُم بِظُلْمٍ أُولَئِكَ لَهُمُ الْأَمْنُ وَهُم مُّهْتَدُونَ)(2). وقال في محكم آياته الكريمة: (وَلَيُبَدِّلَنَّهُم مِّن بَعْدِ خَوْفِهِمْ أَمْنًا)(3).

وفي مفهومه الشامل على مستوى الفرد أو الجماعة أو الدولة فإن الأمن يستوعب الحياة الإنسانية المادة والقيم والفكر.

---

(1) سورة قريش – الآية: من 1 إلى 4.

(2) سورة الانعام – الآية: 82.

(3) سورة النور – الآية: 55.

## المطلب الأول

## مفهوم الأمن

**أ - في اللغة:**

إن كلمة الأمن تعنى من المعانى الكثير، أمن (الأمان) و (الأمانةُ) بمعنى وقد أمن من باب فهم وسلم، وآمنة غيره من الأمن والامان، و (الإيمان) التصديق، والله تعالى (المؤمن) لأنه (آمن) عباده من ان يظلمهم، والأمن ضد الخوف و (الأمنة) هى الأمن ومنه قوله تعالى (آمنة نعاساً)، وقوله تعالى (وهذا البلد الأمين). قال الاخفش: يريد البلد الأمن وهو من الأمن(1). و (أمن منه) مثل (سلَم) منه وزناً ومعنى الأصل استعمال اللفظ آمن فى سكون القلب، و (أمنَ) البلد اطمأن به أهله، وعن حسن البصرى أنه اسم من أسماء الله تعالى. و (آمنت) على الدعاء (تأميناً) قلت عنده (آمين)، و (أستأمنه) طلب منه الأمان، و (أستأمن) إليه دخل فى أمانة(2). هذا معنى الأمن فى اللغة العربية.

**ب- عن مفهوم الأمن اصطلاحاً:**

فإنه يتكامل هذا المفهوم بالنظر إليه من عدة زوايا حتى يمكن توفير هذه القيمة العليا التى بحق تعتبر ضرورة من ضرورات حياة الإنسان وليس مجرد حق من حقوقه يفرض على جهة ما واجبات توفيره(3). ويمكن أن ننظر إلى مفهوم الأمن من زاويتين مختلفتين، ولكنهما فى نفس الوقت متوازيتين ومتكاملتين: أما بوصفه مفهوم شعورى أو على أنه اجراء ضرورى، وذلك على النحو التالى:

---

(١) مختار الصحاح – باب الهمزة – فصل الميم – ص ١٠.

(٢) المصباح المنير – كتاب الألف – ص ٢٤.

(٣) لواء د/ عصمت عدلى – علم الإجتماع الأمنى (الأمن والمجتمع) – دار المعرفة الجامعية – الإسكندرية – سنة ٢٠٠٣، ص ٢٧.

**١- الأمن الشعوري:**

هو احساس الفرد والجماعة باشباع دوافعهما العضوية والنفسية التى تدور حولها احتياجاتها الاساسية وفى مقدمتها دافع الأمن بمظهريه المادى والنفسى، وهو ما يمكن أن يؤدى إلى السكينة العامة أو فى تعبير آخر الهدوء والاستقرار الداخلى.

ولا شك أن هذا الجانب الشعورى من الأمن ذو طبيعة هلامية ومظهر سلبى لا يمكن قياسه مباشرة، وإنما من خلال مؤشرات خارجة عنه تحيط به، ومن أبرزها قياس اتجاهات الرأى العام، ومدى توفر السكينة العامة التى تتمثل فى استقرار وازدهار الحياة الاقتصادية والاجتماعية والثقافية وهكذا[١].

أما اضطراب الأمن الشعورى فيشكل من وجهة النظر العلمية نوعاً من افتقاد أو تعويق أو احباط الاشباع المناسب لحاجات الفرد أو الجماعة ومنها الحاجة للأمن، ويخلق بالتالى اتجاهات عدائية أو جماعية تشكل تناقضاً داخلياً فى المجتمع[٢].

**٢- الأمن الإجرائي:**

هو الجهد المنظم الذى يصدر عن الجماعة لإشباع دوافع أفرادها ورد العدوان عنهم أو عن كيان الجماعة، وتضطلع به السلطة فى حدود نظامها القانونى، وهو بهذا المعنى يتجاوز بكثير المفهوم الضيق للإجراء الأمنى لأنه يمتد إلى كافة مجالات ترشيد وتقويم السلوك الفردى والاجتماعى ليحتوى - بالتالى - على كل ما من شأنه - بالضرورة - تعميق للاتجاهات التربوية والأنماط الثقافية والفنية ووسائل التأثير على الرأى العام من صحافة وإعلام، وعلى هذا الاساس فإن الجانب العقابى فى هذا المفهوم الإجرائى لا يمثل إلاّ

(١) المرجع نفسه - ص ٣٠.

(٢) المؤتمر الأول لوزراء الداخلية العرب (مفهوم الأمن الداخلى فى العالم العربى والتهديدات الموجة إليه) ورقة عمل مقدمة من وفد مصر - القاهرة - سبتمبر ١٩٧٧ - ص ٢٨١.

واحداً من جوانب متعددة يشملها[1]، بالإضافة إلى أنه يمكن القول أن العديد من أجهزة الخدمات المختلفة في الدولة تلعب ادواراً متفاوتة وأساسية في خدمة المفهوم الأمني، وعلى الرغم من ذلك فإن مسئولية استتباب الأمن تقع على عاتق أجهزته التخصصية فقط.

والواقع أنه لا يمكن الفصل بين مفهومي الأمن (الشعوري والإجرائي)، لأن حالة الأمن التي تصبوا إليها كل دولة قائمة على التكامل والاتساق بين هذين الجناحين وهو ما يطلق عليه الاتصال العضوي بينهما، ولكن ليس معنى هذا أن يكون علاج أي اضطراب شعوري بالأمن متجسداً في اجراءات أمنية، لأن زيادة الاخيرة في بعض الحالات قد تؤدي في حد ذاتها إلى تعميق الشعور بوجود اختلال بالأمن لدى الأفراد، وإنما الواقع ان التكامل بينهما تقديري ويخضع لحسابات متعددة تأتي في مقدمتها الرؤية والحس السياسي بمدى الاضطراب الواقع ومسبباته، ومدى تأثيره على تفاقم الموقف أو تداعيه، ومدى السرعة المطلوبة في حسمه[2].

**٣- الأمن القومي:**

إن هدف ا لدولة من ممارسة نشاطها هو خلق الظروف التي يمكن أن يصل فيها أفراد شعبها إلى الحد الأقصى لإشباع حاجاتهم، وتتحدد وظائف الدولة في حماية الاستقلال، وحفظ الأمن الداخلي واشباع حاجات الشعب، وتحقيق رفاهيته من خلال ممارسة نشاطاتها المختلفة ورقابة الأنشطة المؤدية إليها. تمثل صياغة لحاجات المجتمع المختلفة والمتشعبة، كما تعكس المصالح المشتركة وتمثل في نفس الوقت المظهر المادي للسلوك الوظيفي للدولة[3].

---

(١) المرجع نفسه – ص ٢٨٣.

(٢) لواء د/ عصمت عدلي – المرجع السابق – ص ٣٣.

(٣) المؤتمر الأول لوزارء الداخلية العرب – المرجع السابق – ص ٢٨٤.

وفى هذا الإطار وفى حدود المفهوم السابق للأمن فإن فكرة الأمن القومى تدور ببساطة حول أمن الوطن والمواطن. لأن أى اضرار بأحد أنشطة الدولة ينعكس عليها وعلى أفرادها بالضرورة. ويمكن تعريف الأمن القومي من خلال معنى اجرائى شامل بهدف التحديد والوضوح بأنه: (الجهد اليومى الذى يصدر من الدولة لتنمية ودعم أنشطتها الرئيسية السياسية والاقتصادية والاجتماعية، ودفع أى تهديد أو تعويق أو اضرار بتلك الأنشطة)(١).

**٤- الأمن الداخلي:**

هو مجموعة الجهود المبذولة لحماية النظام وأسرار الدولة من النشاط الموجه ضدها من داخل البلاد وخارجها، وتهيئة العوامل الكفيلة بتحقيق وتعميق الشعور بالأمن لدى المواطنين والمجتمع، وإذا كانت جهود الأمن القومى تتسم بصفة عامة بطابع ايجابى أو هجومى، فإن البعض كان يرى أن جهود الأمن الداخلى تتخذ طابعاً دفاعياً (نشطاً)، إلا أن هذه الرؤية بدأت فى التغير تدريجياً فى ظل المفاهيم الحديثة التى تسود الأنظمة المعاصرة لتأخذ فى الجانب الأكبر منها نفس الطابع الإيجابى والهجومى الذى تتسم به جهود الأمن الخارجى(٢).

- **مفهوم الأمن الداخلي:** انطلاقاً من مضمون وظيفة الداخلى فأنه اصطلح على النظر إليه من خلال مفهومين هما: الأمن السياسى والأمن الجنائى – أو العام –، إلا أن كلا الجانبين يمثلان وجهين لعملة واحدة، فأثارهما متكاملة وتأثيراتهما متبادلة، وانعكاساتهما على الاستقرار الداخلى كل لا يتجزأ.

أ - **الأمن السياسي:** هو مصطلح يطلق على الجهود المبذولة للمحافظة على أسرار الدولة وسلامتها. والعمل على منع ما فى شأنه افساد العلاقة بين السلطة

---

(١) عبر (هنرى كيسنجر) وزير الخارجية الأمريكى الأسبق بأن الأمن القومى هو (أى تصرفات يسعى المجتمع من خلالها إلى تأكيد حقه فى البقاء). لواء د/ عصمت عدلى – المرجع السابق – ص ٣٤.

(٢) محمد المرقى – الشرطة فى مواجهة الجريمة – القاهرة – دار القاهرة للطباعة والنشر – سنة ١٩٧٧ – ص ٧٦.

والشعب أو تشويه صورة السلطة لدى الشعب، أى أن الأمن السياسى يقوم على منع وضبط الجرائم الضارة بأمن الدولة من الداخل والخارج إلى جانب التصدى للمشكلات والانحرافات التى من شأنها أن تشكل دوافع ومنطلقات لاثارة الجماهير، وركائز تستند إليها حركة الأنشطة المضادة(١).

ب- **الأمن الجنائي (العام)**: يتمثل فى جهود الدولة لتعميق الشعور بالأمن لدى المواطنين، والعمل على منع أو التقليل من فرص ارتكاب الجريمة وتتبع مرتكبيها وضبطهم وجمع أدلة أدانتهم لتقديمهم للعدالة ومحاكمتهم.

ان قاعدة (**الأمن لا يتجزا**) واردة فى علاقة التكامل والتأثير المتبادل بين الأمن السياسى والأمن الجنائى، لأن السلوك الشاذ أو المنحرف ما دام قد ترك اثراً فى مشاعر الأفراد لابد أن ينعكس بالضرورة على المجتمع الذى يعيشون فيه، أى أنه يمس أمن الفرد وأمن الدولة فى الوقت نفسه، وعلى الجانب الآخر فإن الاجراء الأمنى فى المجال الجنائى يخدم بالضرورة مقومات الأمن السياسى، فمرور الدوريات النظامية على سبيل المثال يخدم اغراض الأمن الجنائى والسياسى على قدم المساواة، وجهود أجهزة الشرطة المتخصصة فى مجالات الجوازات والأحوال المدنية والنقل والمواصلات والتموين إلى غير ذلك، يساعد على تعميق الأمن الشعورى لدى المواطنين، ويمثل بالتالى دعماً لمعالم الاستقرار الداخلى للمجتمع(٢).

إن مفهوم الأمن بكل ما يشمله من معانى متعددة وزوايا مختلفة، يعنى فى واقع الأمر توفير الحماية والطمأنينة والأمان لأفراد المجتمع، من خطر قد يتحقق أو من المتوقع حدوثه، وقد تطور مفهوم الأمن ليشمل توفير الحماية والطمأنينة والأمن والاستقرار النفسى والاكتفاء المادى لأفراد المجتمع من الاحتياجات الغذائية والصحية والروحية والاجتماعية، وهذا هو الأمن الشامل الذى يعكس قدرة المجتمع على التحديات الخارجية، وتحقيق أكبر قدر ممكن من الاكتفاء

---

(١) محمد المرقى – المرجع السابق – ص ٧٧.

(٢) لواء دكتور/ عصمت عدلى – المرجع السابق – ص ٣٧.

الذاتى لضمان الاستقرار للمجتمع، فمسئولية تحقيق الأمن المطلوب بأشكاله المتعددة ليست مسئولية فرد أو مؤسسة بل هى مسئولية جماعية مشتركة، هى مسئولية أبناء المجتمع جميعهم مشاركة مع مؤسسات الدولة المختصة، لأن الأمن فى كل صوره ومعانيه هدف للجميع.

## المطلب الثاني

## من تعريفات الأمن

الأمن هو الإحساس الذى يتملك الإنسان بالتحرر من الخوف، من أى خطر يواجهه[1].

أو الشعور بالطمأنينة الذى يتحقق من خلال رعاية الفرد والجماعة، ووقايتها من الخروج على قواعد الضبط الاجتماعى، من خلال ممارسة الدور الوقائى والقمعى والعلاجى الكفيل بتحقيق هذه المشاعر[2].

كما يعرف الأمن بأنه الادراك الذاتى للفرد والجماعة الإنسانية باختلاف صورها، بالطمأنينة والاستقرار والسكينة، والبعد عن الأخطار والمخاطر، وعن كل ما يهدد الفرد فى نفسه وجسده وعرضه وما له، وما يهدد المجتمع فى استقراره وتقدمه[3].

هذا ما ذهب إليه جانب من الباحثين والمختصين فى مجال الأمن، حيث تركز مفهوم الأمن لديهم على الأحساس أو الشعور أو الادراك الذاتى، وجميعها مترادفات معبرة عن أمن الفرد – الذات الإنسانية – تتجمع لتحقق أمن الجماعة ثم أمن المجتمع، الذى يعتبر الفرد والجماعة من الوحدات المكونة له، والمعبرة عن فئاته (طبقاته).

(١) لواء/ نشأت عثمان خلالى – الأمن الجماعى الدولى – دار المعارف – القاهرة – بدون سنة نشر – ص ١٥٥.

(٢) د/ عماد حسين عبد الله – الأمن فى المدن الكبرى – المركز العربى للدراسات الأمنية – الرياض – سنة ١٩٩٠ – ص ٢٧.

(٣) محمد غالب بكزاده – الأمن وادارة المؤتمرات (النضرية والتطبيق) – دار الفجر للنشر – القاهرة – سنة ١٩٩٨ – ص ٢٤.

وأيضاً ذهب الدكتور/ أحمد هيكل - وزير الثقافة الأسبق - إلى أن مفاهيم الأمن والعدالة ترتكز على أسس إنسانية، تسمو نحو تعميق القيم والأنساق الأخلاقية فكرياً ووجدانياً، ومفاهيم الحق والخير(١).

وفي عرض الدكتور/ بهاء الدين إبراهيم لمفهوم الأمن الداخلي سطر أن الجريمة وإن كانت ترتبط بالأمن العام من بعض الزوايا. فهي في نهاية الأمر مفهوم يختلف كل الاختلاف لأنها شئ مادي، والأمن في حد ذاته إحساس نفسي... الأمن شعور داخلي بالطمأنينة، فإدراك الأفراد بأن هناك سلطة أعلى وأقوى تستطيع أن تحافظ على أرواحهم وأموالهم، وتردع أعداء المجتمع وتقتص منهم، فهذا يوفر لهم السكينة ويضمن لهم الأمان(٢).

ونخلص من ما سبق الى تعريف مقترح للأمن بأنه:

بسط القانون وتطبيقه وسيادته، وردع الخارج عن الشرعية المخالف للنظام القانوني، لليتحقق الشعور بالأمن لدى الفرد ويتكامل مع احساس الآخرين فيتحقق أمن المجتمع.

فسبط القانون يمثل المظهر الخارجي لمفهوم الأمن، حيث يمثل بسيط القانون هدف وطني وقومي يهم جميع مؤسسات المجتمع وأفراده-Law Enforce ment Procedures، ويساعده على تحقيق أهدافه في الاستقرار والأمن الذي يوفر التقدم والتنمية والرخاء. وشعور المواطن بالسكينة وإدراكة لأهمية الالتزام بالقانون واحترام نصوصه، يمثل المظهر الداخلي - النفسي - لمفهوم الأمن.

حيث أن المجتمع المضطرب أمنه، هو الذي يخفت فيه صوت القانون،

---

(١) تقديم د/ أحمد هيكل لكتاب اللواء د/ بهاء الدين ابراهيم محمود - الشرطة والأمن الداخلي (في مصر القديمة) - طبع ونشر هيئة الآثار المصرية - وزارة الثقافة - القاهرة - سنة ١٩٨٦ - ص ٤.

(٢) المرجع السابق - ص ٣.

ويهتز فيه النظام بأجهزته وتضعف سلطة الدولة، فلا تستطيع أن توفر الحماية ولا أن تفرض الأمن والطمأنية، ولا أن تشعر مواطنيها بالأمان.

• **الأمن الذكي:**

سيطرت على بعض المصطلحات الأمنية - بعد أحداث ١١ سبتمبر - عمليات إلصاق صفة الذكاء عليها، وأهم هذه المصطلحات(*):

الدراسات الذكية، الاستخبارات الذكية، القنابل الذكية، العقوبات الذكية(**).

---

(*) طور العلماء واللغويون علماً جديداً أطلق عليه اسم (علم المصطلح) أو المصطلحية وهو العلم الذى يبحث فى العلاقة بين المفاهيم العلمية والمصطلحات اللغوية التى تعبر عنها، وهو علم مشترك بين علوم اللغة والمنطق والإعلام وحقول التخصص العلمي. وقد كان هذا التطور من منطلق ما شهده العالم من طفرة هائلة فى العلوم والتكنولوجيا، والنمو السريع فى المعلوماتية والتعاون الدولى فى شتى المجالات واستخدام الحاسبات الإلكترونية فى خزن المصطلحات ومعالجتها وتنسيقها، ولم تعد الطريقة القديمة فى جمعها وترتيبها أبجدياً ووضع مقابلاتها فى اللغات الأخرى وافية لمواكبة المتغيرات اليومية. وينقسم علم المصطلح إلى نظامين:

**الأول - (عام):** يقوم على البحث فى المفاهيم والمصطلحات التى تعبر عنها، وتستخدم نتائج البحوث فى هذه النظرية بوصفها أساساً لتطوير المبادئ المعجمية المصطلحية وتوحيدها على النطاق العالمى.

**الثاني - (خاص):** يهتم بالنظريات الخاصة للمصطلحية التى تصف المبادئ، التى تحكم وضع المصطلح فى حقول المعرفة المتخصصة كالكيمياء والأحياء والطب.

ومن هنا يمكن أن يطلق علم المصطلح الأمنى على أحد فروع علم المصطلح الخاص بعلم محدد يبحث فى جميع الفعاليات المتصلة بجميع المصطلحات الأمنية وتحليلها وتنسيقها بمعرفة مرادفاتها وتعريفاتها باللغة ذاتها. (د/ على القاسمى - مقدمة فى علم المصطلح - مكتبة النهضة المصرية - القاهرة - ط ٢ - سنة ١٩٩٧ - ص ١٧ وما بعدها).

(**) الدراسات الذكية - هى التى تعطى رؤية مستقبلية وفقاً للاستراتيجية العامة للدولة وأهمها الدراسات الخاصة بخطة معينة تنفذ على مستوى الوزارات أو الهيئات أو الشركات، خطة مستقبلية تشمل كافة جوانب الموضوع التى تتناوله.

• الاستخبارات الذكية - هى التى تعمل فى اطار عولمة المخابرات لمكافحة الارهاب، والهدف منها تفكيك جميع شبكات الارهاب على مستوى العالم، والمحدد لها فترة زمنية قد تتجاوز عشر سنوات.

-/-

والقاسم المشترك بين هذه المصطلحات هو دلالة الذكاء الذى تم أصباغة على كلاً منها، لكى تنفرد عما سبق لها من حالات مماثلة.

وقد امتدت هذه المفاهيم إلى الأمن حيث أطلق على أحدث الدراسات الأمنية لفظ الذكية أو المستقبلية، والتى أصبحت ضرورية لا يمكن الاستغناء عنها، لتوفير إطار زمنى طويل المدى لما قد يتخذ من قرارات يضفى عليها طابع مستقبلى معتمد على أسلوب التفكير، وذلك علامة من علامات النضج العقلى والبلوغ الفكرى فى اتخاذ القرارات، تساعد فى استطلاع النتائج وتوقع التداعيات على مسار المستقبل للأسهام فى تشكيله، كما وأن هذه الدراسات ضرورية للقضاء على عناصر الفقر ومظاهر التخلف.

وانطلاقاً من ذلك يمكن تحديد مسار هذه الدراسات الذكية (المستقبلية) الأمنية فى أنها: (عمل من أعمال الفكر للتركيز على فحص المستقبل، وتقيمة ودراسة صوره وأسسه المعرفية والأخلاقية). وتفسير الماضى وتوجيه الحاضر، وإحداث عمليات تكاملية بين المعارف المتنوعة والقيم المختلفة، وزيادة مشاركة الديمقراطية والبحث العلمى فى تصور وتصميم المستقبل. وقد أطلق على أجهزة الأمن فى الدول التى تعتمد استراتيجيتها الأمنية على دراسات ذكية مستقبلية مصطلح (الأمن الغالى)، وفى الدول التى لا تستخدمها مصطلح (الأمن

---

- القنابل الذكية – هى القنابل التى تطلق من الطائرات لكى تصل إلى الهدف داخل الكهوف والمغارات حتى يصيب الغرض منها. (مثل تلك التى صنعت خصيصاً حتى تتلاءم مع تضاريس أفغانستان).
- العقوبات الذكية – هى التى تحقق أهدافاً استراتيجية، وتمنع الدولة من استمرار مخالفتها للمجتمع الدولى. (ويتمثل ذلك فى إعادة بناء ترسانة أسلحة كيماوية أو بيولوجية أو نووية، مثل الخطر الذى فرض على العراق وأفرز عن اتفاقيات النفط مقابل الغذاء). للمزيد يراجع:

(د/ وحيد عبد المجيد – الإرهاب وأمريكا والإسلام من يطفئ النار – دار المحروسة – القاهرة – ط ١ – سنة ٢٠٠٢ – ص ١٩).

الرخيص) . والغالى والرخيص هنا لا يرتبطان بميزانية ونقود، بل بعمليات بحث علمى راق، ومعيار التفرقة بين الأمن الغالى والأمن الرخيص هنا هو الاعتماد على منهجية الدراسات المستقبلية وأدواتها(١) .

ونظراً للتطورات الهائلة التى تشهدها أنظمة المعلوماتية، فإنه من الأهمية مواءمة أنظمة الأمن الذكى لما يحدث من تقدم وتطور، وذلك عبر تطوير لعمليات البحث العلمى الأمنى، وتحويله من آليات نظرية إلى عملية مرتبطة بالواقع (الأمن الواقعى الفعلى) الذى يقوم على تقديم العلاج بجانب المكافحة فى اطار من الشرعية القانونية ومشروعية الإجراء، حيث أفرزت تكنولوجيا المعلومات – بعضاً من جانبها المظلم السئ – نوعاً من الاجرام الدولى وتدويل النشاط الإجرامى عبر القارات، وأصبح الاتحاد فى مجال الجريمة وارتكابها على غرار نظام (الكارتل الاقتصادى)، مما أدى إلى ظهور مصطلح أطلق عليه (المنظمات الإجرامية غير الوطنية) وهى التى ترتكب الجرائم العابرة للقارات، وتنسف أسس النظام العالمى سواء فى جانبه الاقتصادى أو الاجتماعى أو الاخلاقى، كما أمتد الأمر ليشمل الجوانب السياسية الدولية – من فساد حكام وانحراف قادة – مما ينزر بحقبة شؤم تهدد فيها حقوق الإنسان وتنتهك أدميته .

وبعد .. فإنه يمكن أن نضيف عدة تصورات لمفهوم الأمن، حيث يمكن تصور مفاهيم متباينة للأمن فى ضوء العلاقات الدولية المتباينة كذلك، وخاصة فى ضوء عمليات التغير السياسى والاجتماعى فى البلدان النامية بالذات(٢) . كما قد يفهم من المدرسة الوضعية باعتبارها تركز فقط على عنصر القوة للدولة(٣)،

---

(١) لواء/ عادل عبد العليم – علم المصطلح الأمنى الجديد بعد أحداث ١١ سبتمبر – مقالة بمجلة مركز بحوث الشرطة – أكاديمية مبارك للأمن – القاهرة – العدد ٢٢ – يوليو ٢٠٠٢ – ص٢٣٠ .

(2) Louis A. Radelet: The Police and the Community. Fourth Edition Macmillan Publishing Company, New York, 1989, p. 34.

(٣) بناء على فكر ساد فى أدبيات الأمن القومى أن النظام الأمنى الدولى عموماً هو نظام يتصف بالفوضى بإعتباره نظاماً قائماً على الصراع والتصارع أكثر من قيامه على التعاون. وقد ساهم -/-

تضادها للتحولات الإقتصادية والاجتماعية التى يمر بها المجتمع، حيث تكون هناك إستحالة منطقبة وعملية لأى نظام نام لأن يحقق أى قدر من الأمن... وعلى ذلك فإن مفهوم الأمن فى العالم الثالث يتمثل فى حماية النظام النامى أو هو (عملية توفير الشروط اللازمة لتحقيق التراكم التطورى للنظام) ... وبالتالى يتركز الأمن فى تنمية موارد الدولة والمحافظة عليها وتنمية قدرات الأفراد الإرتباطية وزيادة كمية الموارد الاقتصادية والاجتماعية والاستراتيجية للدولة – وهو ما ينعكس على التعامل اليومى بين الأفراد وعلاقاتهم الاجتماعية. ويعتمد الأمن بذلك ليس فقط على خلق أجهزة دولة مستقلة بل أيضاً تنمية مؤسسات وأجهزة تتعاون مع نظم متماثلة، وإتاحة الفرص لتوظيف سبل تحقيق الأهداف المرجوة مع الغايات الملائمة للبيئة الداخلية فى علاقة متوازنة بين سلطة الدولة وقدرة الفرد.

ونخلص من ذلك إلى أن جوهر العلاقة القائمة بين الأمن بمفاهيمه المختلفة والمعلوماتية بما تمثله من نظام اتصالات تبادلى حديث، يكمن فى تكفل نظام الأمن فى الدولة بحماية النظام المعلوماتى من انتهاك الغير، سواء كان هذا الغير دولة أو مؤسسة أو فرد. وذلك من خلال اجراءات قانونية وأنظمة تشريعية، بالأضافة لتوفير سبل الاستقرار السياسى والاقتصادى من أجل تنمية أنظمة المعلوماتية.

---

= هذا الفكر فى تأسيس كثير من مفاهيم الأمن، خاصة مفهوم معضلة الأمن Security dil-lemma التى قال بها (جون هيرز)، والموقف التفاوضى والتفرقة بين الدفاع والردع الذى قال به (جلين سنيدر)، ومفهوم جوهر الأمن The Essence of security لمكنمارا. ومفهوم الدولة الحصن الذى قال (هارولد لاسل The Garrison State and the Specialista of Violence. وغيرها من المفاهيم الأخرى مثل السيادة الاقتصادية لكل من (هولن ولبوك)، والتى تعرضت لكثير من الإنتقادات الفكرية باعتبارها تمثل المدرسة الوضعية فى العلاقات بين الأطراف المختلفة على أساس أنها مفاهيم (استاتيكية)، (لواء د/ عصمت عدلى – مرجع سابق – ص ٢٨).

## المبحث الثاني
## ماهيـــة المعلوماتية

المعلوماتيـة فكـرة واسـعـة، ولهـا قـوانينهـا الضـابطة، وفـهم العـلاقـة بين المعلوماتية ونظم البرمجيات – بما تشمله من حواسيب واتصالات بعديه – يثير أهمية عرض مفهوم المعلومات ثم التعريف بالمعلوماتية وسماتها. ثم عرض عناصر المعلوماتية التى من خلالها يمكن الاستفادة من التقنيات الحديثة فى النظم والبيانات.

### المطلب الأول
### التعريف بالمعلوماتية

تثير فكرة المعلوماتية قلقاً بالغاً إذا إستخدمت أنظمة المعلومات فى مجالات غير قانونية، وأضحت من عناصر انتهاك الحقوق والحريات العامة، وتعنى المعلوماتية علم التعامل المنطقى مع المعلومات(*)، باعتبارها ناقلة للمعارف الإنسانية، سواء كانت ذات صبغة تقنية أو اقتصادية أو اجتماعية أو سياسية، وذلك من خلال أجهزة ذات تقنية حديثة.

والمعلوماتية لها قواعد ضابطة ونصوص منظمة لاستخدام نظمها، نلمسها بين النصوص القانونية العامة. وعلى ذلك يمكن القول بأن المعلوماتية تخضع لقانون هو: «مجموعة القواعد والأحكام القائمة فى شتى فروع القانون، والتى يمكن تطبيقها على أى مشكلة معلوماتية، بحسب نوع وأركان المشكلة المثارة، والتى قد تخضع لأحكام قانونية عديدة».

---

(*) حيث أن المعلومات عبارة عن بيانات خضعت للتحليل والتفسير، ومن ثم التشغيل والإنتاج، لتحقيق أصول المعرفة وزيادة الفهم للمستفيد (متخذ القرار)، ومساعدته فى تحقيق أهداف وغايات معينة، وتمكينه من الإدارة الناجحة والحكم السليم على معطيات الأمور. فالمعلومات نتيجة أولية أو نهائية يمكن استنتاجها – الوصول إليها – من تشغيل البيانات، أو تحليلها أو استنتاجها، على نحو يثرى المعرفة والعلم للمتسفيد.

## الفرع الأول

## عن المعلومات والبيانات

إن تعريف المعلومات على الرغم مما قد يبدو من أنه لا يثير صعوبة، حيث أن المعلومات تحيط بنا من كل جانب كما أنها تتعلق بكافة مجالات الحياة، إلا أنه يمكن القول أن المعلومات قد اكتسبت بظهور تكنولوجيا الحاسبات الآلية بعداً جديداً أضفى عليها أهمية تفوق ما كانت عليه قبل ذلك، وأكسبها شكلا جديداً، بل تسمية جديدة حيث أصبح يشار إليها بالمعلوماتية إشارة إلى ارتباطها بهذه التكولوجيا الجديدة.

**أولاً: تعريف المعلومات:**

ويمكن تعريف المعلومات بصفة عامة بأنها: «مجموعة من الرموز أو الحقائق أو المفاهيم أو التعليمات التى تصلح لأن تكون محلاً للتبادل والاتصال "Communication" أو للتفسير والتأويل "Interpretation" أو للمعالجة "Processing" سواء بواسطة الأفراد أو الأنظمة الإلكترونية، وهى تتميز بالمرونة بحيث يمكن تغييرها، وتجزئتها، وجمعها، أو نقلها بوسائل وأشكال مختلفة»(1).

ويميز البعض فى تعريف المعلومات بينها وبين البيانات. فالبيانات تعبر عن الأرقام والكلمات والرموز أو الحقائق أو الإحصائات الخام التى لا علاقة بين بعضها البعض، ولم تخضع بعد للتفسير أو التجهيز للإستخدام، والتى تخلو من المعنى الظاهر فى أغلب الأحيان، أما ا لمعلومات فهى المعنى الذى يستخلص من هذه البيانات(2).

---

(1) Parker (Donn B.): Figting computer crime "A New Framework For Protecting Information. 1998. p. 27.

(٢) د/ نائلة عادل محمد فريد قورة – جرائم الحاسب الاقتصادية – منشورات الحلبى القانونية – القاهرة – سنة ٢٠٠٥ – ص ٩٤.

– ويدلل البعض على هذه التفرقة بالمثال التالى: إن عبارة "Le soleil Brille" باللغة الفرنسية على سبيل المثال، تعنى أن الشمس مشرقة وهى لا تعدو أن تكون بياناً لحالة الشمس، ولا يمكن

-/-

والواقع أننا لا نجد جدوى من التمييز بين المعلومات والبيانات فى مقام دراستنا فالذى يعنينا فى هذا المقام هو حماية المعلومات بصفة عامة وطالما أن المعلومات هى المعنى المستخلص من البيانات، فالحماية تشملهما معاً، ومن ناحية أخرى قد لا تكون المعلومة مفهومة لدى متلقيها وهو ما يجعلها تخرج عن دائرة المعلومات طبقاً لهذه التفرقة ورغم ذلك يكون الوصول إليها والتلاعب بها على قدر كبير من الخطورة، فالذى يعنينا هو حماية المعلومات بغض النظر عن فهم محتواها. ولذلك فنحن نفضل استخدام المعلومات والبيانات فى هذا المقام كمترادفين(١).

وتتميز المعلومات بصفة عامة بقابليتها للدمج، فقد تضاف معلومة إلى أخرى لتكونا معاً معلومة جديدة تختلف قيمتها وأهميتها، وبالتالى فى مقدار الحماية اللازمة لها عما كانت عليه قبل عملية الدمج(*)، فلكل معلومة إذاً قيمة

---

= أن تتحول إلى معلومة لدى أحد الأشخاص إلا بشرطين: الأول أن يطلع عليها بالفعل. والثانى أن يكون هذا الشخص على علم باللغة الفرنسية حتى يستطيع أن يتفهمها. وحتى يتحقق هذان الشرطان تظل البيانات مجموعة من الحروف، ولا يمكن أن تتحول إلى معلومة إلا بتوافرهما.
وقد أخذت التوصية الصادرة عن منظمة التعاون الاقتصادى والتنمية عام ١٩٩٢ الخاصة بحماية أنظمة الحاسبات الآلية وشبكات المعلومات، بالتفرقة السابقة حيث عرفت البيانات بأنها مجموعة من الحقائق أو المفاهيم أو التعليمات تتخذ شكلاً محدداً يجعلها قابلة للتبادل وللتفسير أو للمعالجة بواسطة الأفراد أو بوسائل إلكترونية. أما المعلومات فهى المعنى المستخلص من هذه البيانات.

- Recommendation of the Couneil Concerning Guidelines for the Security of Information System, 26 November, 1992.

(١) د/ نائلة عادل محمد قورة – المرجع السابق – ص ٩٥.

(*) فعلى سبيل المثال رقم حساب عميل فى البنك معلومة على قدر من الأهمية وتحتاج هذه المعلومة بطبيعة الحال إلى حمايتها، إلا أنه إذا أضفنا إلى هذه المعلومة معلومة أخرى كاسم البنك واسم العميل وحجم الرصيد فإن قيمة المعلومة وأهميتها فى هذه الحالة تتضاعف وتتطلب من ناحية أخرى قدراً أكبر من الحماية.
ويرجع لهذا السبب قيام البنوك بإرسال كل معلومة على حدة عن طريق عمليات اتصال مختلفة فهى تقوم على سبيل المثال بإرسال مجموعة كبيرة من أرقام الحسابات عن طريق عملية اتصال، وإرسال قيمة الأرصدة عن طريق عملية اتصال أخرى، ويتم تجميع المعلومات المختلفة فى مركز لمعالجتها وذلك بهدف الحفاظ على سرية هذه المعلومات، (د/ نائلة قورة – المرجع السابق – ص ٩٦).

أقل بدون دمجها مع غيرها من المعلومات، على نحو صحيح ليكونوا معاً معلومة أكثر أهمية، فالمعلومات الصغيرة مثل قطع الموازيكو تتكامل لتكون صورة متسقة من المعلومات، وهذا ما يطلق عليه النظرية التكاملية للمعلومات The Mosaic Theory of information[(1)].

**• صفات يلزم توافرها في المعلومات:**

يلزم أن تتوافر فى المعلومة بصفة عامة - سواء أكان التعبير عنها يتم من خلال وسيط مادى أم كانت بمعزل عن هذا الوسيط - بعض الصفات حتى يمكن أن تتمتع بالحماية القانونية. وتتمثل هذه الصفات فيما يلى:

**١- أن تكون المعلومة محددة ومبتكرة[(٢)]:**

إن المعلومة التى تفتقر لصفة التحديد لا يمكن أن تكون معلومة حقيقية. فإذا كانت المعلومة هى تعبير وصياغة محددة تجعل رسالة ما قابلة للتبليغ والتبادل عن طريق علامات أو إشارات مختارة[(٣)]، فينبغى أن تكون محددة. فالمعلومة المحددة هي التي يمكن حصرها فى دائرة خاصة بها، وتحديد جوانبها، وهو ما يعد ضرورياً فى حالة الاعتداء على الأموال، لأن هذا الاعتداء يجب أن ينصب على شئ محدد، وأن يكون هذا الشئ بدوره محلاً لحق محدد[(٤)].

---

(1) Parker (Donn), Op. cit., p. 28.

(٢) د/ عبد العظيم مرسى الوزير - شرح قانون العقوبات (القسم الخاص) - دار النهضة العربية - سنة ١٩٩٣ - ص ٤٠، ٤١؛ د/ نائلة قورة - المرجع السابق - ص ص ١٠٨، ١٠٩.

(3) Catala (Pierre), "Les Transformations de Droit par I'Informatique", in Bensoussan (Alain), Linamt de Bellefonds (Xavier), Maisl (Herbert) (eds.), emergences du Droit de I'Informatique, 1983, p. 264.

(4) Lucas de leyssac (Marie-Paule), Une Information Seule est-elle Susceptible de Vol ou d'Une Autre Atteinte Juridique aux Biens D., 1985, Chr, p. 53.

أما فيما يتعلق بالابتكار "Information Originale"، فإنه ينبغي أن تنصب هذه الصفة على الرسالة التى تحملها المعلومة، فمعلومة غير مبتكرة، هى معلومة عامة، متاحة للجميع، ولا يمكن نسبتها إلى شخص محدد، أو طائفة من الأشخاص، وتبدو أهمية هذه الرابطة عند تناولنا للصفتين التاليتين: (السرية والاستئثار).

**٢- أن تتصف المعلومة السرية والاستئثار:**

كلما اتسمت المعلومة بالسرية "Information Confidentiélle"، كان المجال الذى تتحرك فيه الرسالة التى تحملها، محدداً بمجموعة معينة من الأشخاص. وبدون هذا التحديد فإنه لا يمكن أن تكون المعلومة محلاً يعتدى عليه بالسرقة أو النصب على سبيل المثال، فالمعلومة غير السرية تكون صالحة للتداول، ومن ثم تكون بمنأى عن أى حيازة كالمعلومات التى تتعلق بحقيقة معينة (كحالة الجو فى وقت محدد)، أو بحدث معين، وهى جميعها معلومات تفتقر إلى السرية.

وقد تستمد المعلومة سريتها من طبيعتها (اكتشاف فى أحد المجالات التى تتميز بالسرية)، أو لرغبة صاحبها فى ذلك، أو للسببين معاً كما فى حالة الشفرة السرية الخاصة باستعمال بطاقات الائتمان. وفى جميع الحالات فإن السرية التى تتمتع بها المعلومة هى التى تحدد نطاق استعمالها فى دائرة محددة، بحيث يستفيد أصحابها من الخاصية الثانية، وهى الاستئثار بالمعلومة.

وتعد خاصية الاستئثار بالمعلومة "Information Exclusive"، أمراً ضرورياً، لأنه فى مختلف الجرائم التى تنطوى على اعتداء قانونى على الأموال، فإن الفاعل يعتدى على حق يخص الغير على سبيل الإستئثار، ويتوا فر للمعلومة هذه الصفة، إذا كان الوصول إليها غير مصرح به لأشخاص محددين. إلا أن الاستئثار بالمعلومة قد يرجع إلى سلطة شخص ما على المعلومة فى التصرف فيها، وفى هذه الحالة يكون الاستئثار لمؤلف المعلومة، ويرتبط بهذا الشكل من أشكال الاستئثار بالمعلومة نوع من الرابطة نجدها متحققة فى حالتين:

**الحالة الأولي:** تتعلق بالمعلومات التى ينصب موضوعها على بيان حقيقة أو واقعة ما، وهذا النوع من المعلومات هو بحسب الأصل غير سرى ومتاح للجميع، أما إذا قام شخص بتجميع وحفظ هذه المعلومات ذاتها، فهو ينشأ عن طريق هذا التجميع والحفظ معلومة جديدة، يمكن أن يستأثر بالتصرف فيها بمفرده(1).

وتتحقق **الحالة الثاني:** لتوافر الرابطة بين المعلومة وصاحبها، عندما يكون موضوع هذه المعلومة فكرة أو عمل ذهنى، ففى هذه الحالة ينظر مؤلف المعلومة إليها باعتبارها ملكاً خاصاً له، فإذا تمكن الغير من الاستيلاء عليها، وعلى نحو غير مشروع، فسوف يشعر صاحبها بأنه قد سلب(*).

**ثانياً: تأصيل مصطلح المعلوماتية:**

المعلوماتية أو المعالجة الآلية للمعلومات، هى كلمة مكونة من مقطعين المقطع الأول من كلمة معلومات Information، والمقطع الثانى من كلمة أوتوماتيك أو الى Automatique، وهى كلمة قد لا يستسيغها القارئ العربى للوهلة الأولى. ولكن من الأجدر الأخذ بها لما لها من شيوع فى المجال الدولى(**).

---

(1) Huet (Jérome), "droit Privé et l'Iinformatique", in Bensoussan (Alain), Linant de Bellefonds (Xavier), Maisl (Herbert) (eds.) emergence du Droit de l'Informatique, 1983, p. 33, Lucas De Leyssac (Marie-Paule), Op. cit., p. 44.

(*) ولا تتوافق النصوص القانونية مع هذا الاتجاه، حيث لا تعتد قوانين الملكية الفكرية بالأفكار المجردة، طالما لم تتخذ شكلاً محدداً، كمؤلف على سبيل المثال. وهكذا فإن القانون الفرنسى الصادر عام ١٩٥٧، ويقابلة القانون المصرى الصادر عام ١٩٥٤، يربط حماية الأفكار بوضعها فى شكل معين، وعليه يوفر هذا الشكل للمعلومات الحماية المدنية والجنائية ضد كل تقليد، وهو الأمر الذى لا يتوافر للمعلومات فى ذاتها فى ظل النصوص التقليدية.
أنظر: د/ محمد سامى الشوا، ثورة المعلومات وانعكاساتها على قانون العقوبات – سنة ١٩٩٤– ص١٧٧.

(**) نحت كلمة معلوماتية فى اللغة الفرنسية (informatique) Philippe drefus عام ١٩٦٢ بتجميعه المقطع الأول من كلمة معلومات مع المقطع الأخير من كلمة أوتوماتيك لوصف المعالجة الآلية للمعلومات.

والمعلوماتية مصطلح استعمله لأول مرة A.I.Mikhailov(*)، أسمّ لعلم المعلومات العلمية Science of Scientific Information، ثم ذاع استخدامه بعد ذلك على مستوى جغرافي واسع، بمفاهيم متباينة، حتى أحصى له البعض أكثر من ثلاثين تعريفاً مختلفاً في الكتابات المتخصصة في علم المعلومات(١).

وقد صاغت الأكاديمية الفرنسية تعريفاً للمعلوماتية في جلستها المنعقدة بتاريخ ٦ ابريل سنة ١٩٦٧ – القرن الماضى – سطرته على أنها «علم التعامل العقلانى – على الأخص بواسطة آلات أوتوماتيكية – مع المعلومات باعتبارها دعامة للمعارف الإنسانية وعماداً للإتصالات فى ميادين التقنية والاقتصاد والاجتماع»(٢).

وخطا اليونسكو خطوات أكثر حداثة نحو تعريف موسع لتنمية المعلومات، أو ما اصطلح على تسميته بالمعلوماتية(**)، بينما عند الكثير من الخبراء

---

(*) هو مدير المعهد الاتحادى للمعلومات العلمية والتقنية (Viniti) بالاتحاد السوفيتى (سابقاً)،
- Peter Large, Brove New World? Macdonald, London, 1982, p. 3.

(١) د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات – مكتبة الآلات الحديثة – أسيوط – سنة ١٩٩٤ – ص ٢٧.

(2) Jean - Paul Buffelan, Introduction à L'informatique Juridique, Paris, Librarie du Journal des notaires et des avocats, 1975, p. 16,

وهو يرى أن هذا التعريف غامض وغير كاف، ويفضل عليه تعريف المعلوماتية فإنها، علم المعالجة المنطقية والآلية للمعلومات.
- La science du logique et automatique de L'information.

وتعريفه المقترح قال به فى مرجعه:
- Alain chouraqui, L'informatique au service du droit, Paris, P.U.F., 1974, p. 9.

مشار إليه لدى: د/ هشام محمد فريد رستم – المرجع السابق – ص ٢٨ – هامش (١).

(**) يدرج فى هذا التعريف – مفهوم المعلوماتية – الفروع العلمية والتقنية والهندسية وأساليب الإدارة الفنية، المستخدمة فى تداول ومعالجة المعلومات وفى تطبيقاتها، والمتعلقة كذلك بالحسابات وتفاعلها مع الإنسان والآلات، وما يرتبط بذلك من أمور إجتماعية واقتصادية وثقافية، يراجع:
- Robert Irvine smith and Bob Camp bell: In formation Technology revolution, Long man, 1982, p. 1.

والمختصون تعنى تقنية المعلومات التزاوج والالتحام بين تقنيات الحاسبات والأتصالات والاستعمال المتزايد للالكترونيات، فى العمليات الصناعية والتجارية ابتداء بنظم البرمجيات بالحاسب، حتى بطاقة الائتمان - الدفع الالكترونى - التى يحتفظ بها الشخص معه[1].

• **ثالثاً بيان المصطلحات المعلوماتية:**

فى إطار النظم المعلوماتية وما يتعلق بها من اعتداء يمثل خروج عن الشرعية القانونية ويؤدى إلى الجريمة المعلوماتية وما يتبعها من خرق لنظم الحاسب الآلى، فإنه من الأهمية أن نستعرض بعض من المصطلحات المستخدمة فى هذا النطاق، مسترشدين فى ذلك بما ورد فى اتفاقية بودابست الموقعة فى ٢٣ نوفمقبر ٢٠٠١ بخصوص جرائم المعلوماتية، وذلك على أساس أن التحديد الدقيق الواضح لهذه المصطلحات - المفاهيم - كما وردت فى هذه الاتفاقية وأوضحتها المذكرة التفسيرية، يبدد الغموض ويمنع اللبس، ويساعد مأمور الضبط على الفهم الصحيح لهذه النوعية من الجرائم وذلك حتى يتمكن من مكافحتها بالطرق العلمية والأساليب القانونية السليمة. وقد وردت هذه التعريفات فى المادة الأولى من اتفاقية بودابست ٢٣ نوفمبر ٢٠٠١[2]:

أ - **النظام المعلوماتي Systéme Informatique[3]:**

يعنى كل آلة بمفردها أو مع غيرها من الآلات المتصلة أو المرتبطة والتى يمكن أن تقوم سواء بمفردها أو مع مجموعة عناصر أخرى، تنفيذاً لبرنامج معين بأداء معالجة آلية للبيانات.

---

(١) د/ هشام محمد فريد رستم - المرجع السابق - ص ٢٨.

(٢) د/ هلالى عبد اللاه أحمد - الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١) - مرجع سابق - ص ٤٠ وما بعدها.

(٣) يقابل ذلك فى المصطلح الانجليزى: Computer System

هذا وقد أوضحت المذكرة التفسيرية للاتفاقية بودابست أن المقصود بالنظام المعلوماتي: هو جهاز يتكون من مكونات مادية(١) ومكونات منطقية(٢)، وذلك بغرض المعالجة الآلية للبيانات الرقمية(٣)، وهو يشتمل على وسائل لإدخال(٤) وإخراج(٥) وتخزين(٦) البيانات(٧)، وهذا الجهاز قد يكون منفرداً أو متصلاً بمجموعة من الأجهزة المماثلة عن طريق شبكة،(٨) .

- وكلمة آلية Automatisé : تعني دون تدخل بشري.
- ومعالجة البيانات Le traitement des dannées: تعني مجموعة من

---

(١) مكونات مادية Matériels، ويقابل ذلك في المصطلح الانجليزي Hard ware أي معدات الحاسب المادية أو الصلبة، التي تستخدم في معالجة البيانات وتضم المعدات الآلية والتركيبية الكهربائية التي يتكون منها الحاسب

(٢) مكونات منطقية Logiciels، ويقابل ذلك في المصطلح الانجليزي Soft ware أي المكونات غير المادية للحاسب، أو الكيانات المنطقية، أو البرمجيات، ويقصد بها مجموعة البرامج التي تشكل نظاماً معيناً.

للمزيد بشأن النظام المعلوماتي يراجع:

* د/ عبد الفتاح مراد – موسوعة مصطلحات الكمبيوتر والانترنت – الإسكندرية – بدون ناشر – سنة ٢٠٠٢، مجدى محمد أبو العطا – تيسير Office xp (Microsoft) – القاهرة – العربية لعلوم الحاسب – الطبعة الأولى – سنة ٢٠٠٢، علي يوسف علي – معجم مصطلحات الحاسب – القاهرة – مرجع سابق – ص ٣٢٨ وما بعدها.

(3) Pour Le Traitement automatisé des données muméri ques.

ويقابل ذلك في الطبعة الإنجليزية: For autopmatic Processing of digital data

- see: D,Lura E: Quaran Tieuo, Cyber Crime, How to protect your self from computer criminals. Tiare publications, 1997, p. 139.

(٤) إدخال Des moynes d'acquisiton، ويقابل ذلك في المصطلح الانجليزي In Put.

(٥) إخراج De restitutions، ويقابل ذلك في المصطلح الانجليزي Out put.

(٦) تخزين De stockage، ويقابل ذلك في المصطلح الانجليزي Storage.

(٧) البيانات Donnés، ويقابل ذلك في المصطلح الانجليزي data التي هي لغة جمع لكلمة Datum. وقد جرى العرف على استخدامها مفردا وجمعاً في نفس الوقت، وفي الاصطلاح يقصد بها الوحدة الأولية للمعلومات.

(٨) شبكة un réseau. ويقابل ذلك في المصطلح الانجليزي a net work.

العمليات التى تطبق على البيانات من خلال برنامج معلوماتى Un programme informatiquc [1].

والبرنامج المعلوماتى عبارة عن مجموعة من الأوامر التى يمكن أن تنفذ من خلال الحاسب[2] لتحقيق النتيجة المنشودة، ويمكن لجهاز الحاسب أن يقوم بتشغيل برامج مختلفة.

وفى داخل النظام المعلوماتى يمكن التفرقة عامة بين العديد من المكونات، والتى تعرف باسم المعالج[3] أو وحدة المعالجة الرئيسية L'unité centrale [4]، والوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات[5].

**ب- البيانات المعلوماتية Données informatiques[6]:**

تعنى كل تمثيل للوقائع، أو المعلومات، أو المفاهيم تحت أى شكل، وتكون مهيأة للمعالجة الآلية بما فى ذلك برنامج معد من ذات الطبيعة، يجعل الحاسب يؤدى المهمة.

وتشير المذكرة التفسيرية لاتفاقية بودابست إلى أن تعريف البيانات المعلوماتية الواردة بالفقرة الأولى من هذه الاتفاقية،مأخوذ عن هيئة التوصيف العالمية الأيزو(ISO) (*).

---

(١) ويقابل ذلك فى المصطلح الإنجليزى computer program.

(٢) الحاسب L'ordinateur، ويقابل ذلك فى المصطلح الانجليزى The computer.

(٣) المعالج Le processeur، ويقابل ذلك فى المصطلح الانجليزى The Processor.

(٤) وفى اللغة الانجليزية يطلق عليها Central Processing unit.

(٥) معالجة البيانات Les Periphériques ويقابل ذلك فى المصطلح الانجليزى Peripherals.

(٦) ويقابل ذلك فى المصطلح الانجليزى Computer data.

(*) الحروف الثلاثة (ISO) هى أوائل الكلمات الثلاث التالية:
Internatioal standar dization أى هيئة التوصيف العالمية (الأيزو)، وهى هيئة دولية لوضع المواصفات تمثل فيها الدول بهيئات التوصيف الاقليمية بهدف توحيد المواصفات على المستوى الدولى.

وأن هذا التعريف يتضمن ضمن ما يتضمنه عبارة: (التى تكون مهيأة للمعالجة الآلية (Qui Se Préte a un traitement). وهذا يعنى أن البيانات لابد أن توضع فى شكل يسمح بمعالجتها مباشرة عن طريق الحاسب[1]، ويجب أن يكون معلوماً أن البيانات المعلوماتية التى يتم معالجتها آلياً، يمكن أن تكون هدفاً Lacible لإحدى الجرائم الجنائية التى تستهدف النظام المعلوماتى وأوضحتها هذه الاتفاقية[2].

جـ- **مقدم الخدمة Fournisseur de Service** [3]: يشير إلي:

- كل جهة عامة أو خاصة تقدم لمستخدمى خدماتها إمكانية الاتصال عن طريق النظام المعلوماتى.
- كل جهة أخرى تعالج أو تخزن البيانات المعلوماتية بدلاً من خدمة الاتصال أو نيابة عن مستخدمى هذه الخدمة.

وقد حرصت المذكرة التفسيرية على أن توضح أن تعريف مقدم الخدمة الوارد فى الفقرة (جـ) من المادة الأولى ينطبق على كل من يقوم بخدمات الاتصال Des service de communication[4]، أو خدمات معالجة البيانات... Des services de traitement des données [5] أو خدمات تخزين البيانات... Des services de stockage des données[6]. ويستوى فى ذلك أن تكون الجهة التى تقدم الخدمة جهة عامة أو خاصة، كما يستوى أن تكون

---

(١) من أجل توضيح أكثر لمعنى (البيانات) فى هذه الاتفاقية، أن يتم فهمها على أنها: (بيانات تأخذ شكلاً إليكترونياً، أو أى شكلاً آخر يسمح بمعالجتها مباشرة).

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٤٧.

(٣) ويقابل ذلك فى الطبعة الإنجليزية Service provider.

(٤) ويقابل ذلك فى المصطلح الانجليزى Communication services.

(٥) ويقابل ذلك فى المصطلح الانجليزى Data processing services.

(٦) ويقابل ذلك فى المصطلح الانجليزى Users.

الخدمة مقدمة لمجموعة من المستخدمينUtilisateurs[1] يشكلون جماعة مغلقة أو أنها مقدمة للجمهور، كذلك يستوى أن تكون الخدمة مقابل رسوم أو بالمجان .

**د - البيانات المتعلقة بالمرور Données re latives ou traffic[2]،**

تعنى كل البيانات التى تتعامل مع الاتصال، والتى تمر من خلال النظام المعلوماتى، أو يتم إعدادها بواسطة هذا الأخير، والذى يعد عنصراً فى سلسلة الاتصال، بالإشارة إلى مصدر الاتصال، مكان الوصول، خط السير، الساعة، التاريخ، الحجم، مرة الاتصال، أو نوع الخدمة المؤداة .

وتشير المذكرة التفسيرية إلى أن بيانات المرور المعرفة فى الفقرة (د) من المادة الأولى من الاتفاقية تشكل طائفة من البيانات المعلوماتية الخاضعة لنظام قانون معين. وان هذه البيانات تنشأ عن طريق أجهزة الحاسب فى سلسلة من الاتصالات، من أجل توجيه الاتصال من منبعه أو أصله إلى مكان وصولهDe son orgine a sa destination[3]، وعلى ذلك فهى من ملحقات Des au xiliaires الاتصال فى حد ذاته[4] .

كما تبين المذكرة الإيضاحية أهمية بيانات المرور فى حالة وقوع جريمة جنائية بقولها: «أنه فى حالة التنقيب بخصوص جريمة جنائية ارتكبت فى نظام معلوماتى، فإن بيانات المرور تكون ضرورية من أجل تحديد مصدر الاتصال،

(١) كما ينسحب هذا التعريف أيضاً ليشمل الأشخاص الذين يعرضون خدمة الاستضافة أو التخزين المؤقت (بمعنى الإخفاء)، أو الربط بالشبكة. ولكن لا ينطبق هذا التعريف على مجرد مقدم المحتوى، كأن يتعاقد شخص مع هذا المقدم على إنشاء موقع له على الشبكة العالمية، دون أن يقوم هذا الأخير بأى خدمات كخدمات الاتصال أو المعالجة أو التخزين.

(د/ هلالى عبد اللاه أحمد – المرجع نفسه – ص ٤٨) .

(٢) ويقابل ذلك فى الطبعة الإنجليزية Traffic data .

(٣) ويقابل ذلك فى المصطلح الإنجليزى From its origin to its destination .

(٤) يقابل ذلك فى المصطلح الإنجليزى Auxiliary .

وذلك كنقطة بداية تسمح بتجميع أدلة أخرى، أو جزء من دليل الجريمة، وبيانات المرور يمكن أن تكون سريعة الزوال ولذلك يكون من الضرورى العمل على حفظها فوراً(١).

**رابعاً: الخصائص المميزة للمعلوماتية:**

تتميز المعلومات بصفة عامة بمجموعة من الخصائص التى تساعد على التعرف على طبيعتها وأهميتها وعلى مقدار الحماية اللازمة لها، ويمكن القول بشكل عام أن اكتساب المعلومة لأهميتها يقتضى تحويلها إلى شكل ملموس، حتى يمكن الوقوف على وجودها وبالتالى التمكن من حمايتها. فنحن نتعرف على المعلومة بالإشارة إليها وذكر اسمها، ونتمكن من معرفة وجود ملف ما من قراءة اسمه فى فهرس ملفات البيانات فى الحاسب الآلى "The Computer's file directory" وبالتالى فتح هذا الملف لعرض المعلومات التى يحتويها على شاشة الحاسب. إذا كى تكتسب المعلومة قيمة ما وتكون تبعاً لهذه القيمة جديرة بالحماية ينبغى أن تظهر فى إطار معين يضفى عليها هذه القيمة، ويحدد هذا الإطار مجموعة من الخصائص، والتى تنقسم إلى طائفتين، الأولى: الخصائص الأساسية للمعلومات والثانية: الخصائص التكميلية.

**أ - الخصائص الأساسية للمعلوماتية:**

تنقسم الخصائص الأساسية للمعلوماتية إلى أربع أركان رئيسية هى: نوع المعلومة "Kind" الصورة التى توجد عليها المعلومة "representation" شكل المعلومة "Form" وأخيراً الوسيط المادى الذى يحتوى عليها "Media"(٢).

---

(١) قد يكون من الضرورى الكشف السريع عن بيانات المرور لمعرفة خط سير الاتصال، وتجميع الأدلة قبل أن تمحى، أو من أجل تحديد هوية المشتبه فيه. (د/ هلالى عبد اللاه أحمد - المرجع نفسه - ص ٤٩).

(٢) د/ نائلة قورة - المرجع السابق - ص ٩٧ وما بعدها.

١- النوع:

تختلف المعلومات فيما بينها من حيث النوع وتختلف أهميتها تبعاً لذلك، والمعلومة قد تكون نوعاً من المعرفة، وقد تكون في شكل رسم هندسي، وقد تكون مجموعة من الأوامر والإرشادات، وقد تتعلق بأمور مالية أو على العكس قد تكون ذات طبيعة فنية أو أدبية، أو غير ذلك من مئات الأشكال التي قد توجد المعلومة عليها، ومن بين الأنواع المختلفة للمعلومات سوف نشير فيما يلي إلى أكثرها أهمية:

• المعرفة:

المعرفة "Knowledge" هي نوع من المعلومات يتم اكتسابها عن طريق الخبرة الإنسانية والدراسة، وهي بالتالي تختلف عن ذلك النوع من المعلومات الذي يشر إليه بلفظ "Noledge" والذي لا يمكن معرفته عن طريق الخبرة العادية أو الدراسة، وفي مجال تكنولوجيا المعلومات ينطبق هذا النوع الأخير على كل معلومة يتم استخدامها وتخزينها في الحاسبات الآلية وفي دوائر الاتصالات دون أن يتمكن أي شخص من قراءتها أو معرفتها، فهي في أغلب الحالات لا يهم أي شخص معرفتها في ذاتها - باستثناء بعض المعلومات المشفرة - وإنما تكمن الأهمية في النتائج التي تستخدم هذه المعلومات للوصول إليها، وينطبق هذا النوع من المعلومات - على سبيل المثال - على النتائج التي تتوسط أية عملية حسابية، أي المراحل التي تمر بها العملية الحسابية قبل الوصول إلى النتيجة النهائية، وعلى الثوابت في العلوم الطبيعية والرياضية، كما ينطبق أيضاً على جميع المعلومات المشفرة، وأخيراً فإنه يمكن القول أن هذا النوع من المعلومات يحتفظ به الحاسب الآلي، وذلك من أجل الوصول إلى النوع الأول من المعلومات عندما نحتاج إليه(*).

---

(*) ويتميز كل نوع من النوعان السابقان من المعلومات من حيث القابلية للتلاعب به. فالنوع الثاني "Noledge" أكثر عرضة للتلاعب به من النوع الأول "Knowledge"، وذلك

-/-

● **المعلومات التي تتخذ شكل التعليمات في مجال تكنولوجيا الحاسبات الآلية:**

يكتسب هذا النوع من المعلومات أهمية وقيمة خاصة نظراً لاستخدامها فى مجال الحاسبات الآلية، فالمعلومات فى هذه الحالة والتى تتخذ شكل برامج للحاسب الآلى "Soft ware" تعطى التعليمات اللازمة لتشغيل الحاسب لقيامه بالعمليات المطلوبة منه[1]، ومن ثم كانت هذه البرامج وسيلة مهمة لارتكاب كثير من جرائم المعلوماتية. ومن هنا كانت ضرورة الاهتمام بتوفير الحماية اللازمة لهذه البرامج، ولا يختلف الأمر سواء كانت هذه البرامج مصدرية أو أصلية "Source Program"من ناحية أم كانت برامج هدف "Object Program" من ناحية أخرى، ففى كلتا الحالتين يمكن التلاعب فى البرنامج وتغييره سواء كان هذا التلاعب مقصوداً فى ذاته أم كان المقصود منه ارتكاب جريمة أخرى بمساعدته.

---

= لسببين: صعوبة اكتشاف التلاعب من ناحية وما لهذا التلاعب من تأثير كبير فى كثير من الأحيان من ناحية أخرى. ومن الأمثلة على ذلك ما حدث فى أحد الأبحاث الخاصة بالأسلحة النووية فى سويسرا عندما تمكن أحد الأشخاص من الدخول إلى نظام الحاسب الآلى عن طريق الحاسب الرئيسى، ثم قام بتغيير رقم واحد فى النسبة بين طول محيط الدائرة وقطرها (ويرمز له بلفظ Pi وهو يمثل النسبة بين محيط الدائرة وقطرها أى ٣,١٤١٥٩٢٦٥)، ولقد نتج عن هذا التغيير البسيط والذى لم يتمكن الباحثون من ملاحظته خسائر تقدر بملايين الدولارات نتيجة للنتائج غير الصحيحة التى نجمع عن استخدام نسبة خاطئة لمحيط وقطر الدائرة.

- Parker (Donn), op. cit., p. 33.

وعليه يختلف النوع الأول من المعلومات عن النوع الثانى من حيث أسلوب الحماية، فالنوع الأول يتطلب رقابة على الأفراد وعلى أنظمة الحاسبات الآلية والشبكات على حد سواء طالما أن هذا النوع من المعلومات يمكن الوصول إليه ومعرفته من قبل أى شخص. أما النوع الثانى فإنه يتطلب رقابة على أنظمة الحاسبات وعلى الشبكات بصورة أكبر، فيتعين، من ناحية، التأكد من صحة هذه المعلومات المخزونة فى أنظمة الحاسبات الآلية بصفة دورية، ومن ناحية أخرى، فإنه ينبغ التأكد من عدم وصول أى شخص إلى هذه المعلومات والإطلاع عليها، ويكون ذلك عن طريق تشفيرها ليس للحفاظ على سريتها وإنما لضمان سلامتها (Integrity) والثقة فى صحتها (Authenticity)، على ألا يسمح بفك نظام التشفير إلا فى الحالات التى تقتضى ذلك ولفترة زمنية محددة.

(1) Bing (Jon); Information Law, M.L.P., May 1981, vol, 2, N°.1, p. 223.

ولا توجد صعوبة كبيرة فى اكتشاف التلاعب الذى قد يلحق ببرامج المصدر، على عكس الحال فيما يخص برامج الهدف.

• **المعلومات التي تتعلق بقطاع الأعمال:**

هناك عدة أنواع من المعلومات تتعلق بقطاع الأعمال، وتتمتع بأهمية كبرى وفى حاجة إلى حمايتها من التلاعب بها. وقد تزايد اعتماد هذا القطاع على البرمجة الآلية للمعلومات بشكل كبير. ومن أهم الأمثلة لهذه المعلومات:

- المعلومات التى تتصل بحجم التعاملات وبالعملاء، وتعد هذه المعلومات من أكثر الأنواع حاجة إلى السرية نظراً لأهميتها الشديدة لمنافسى النشاط الذى تتعلق به.

- المعلومات ذات الطبيعة المالية، وهى المعلومات التى تتعلق بالمركز المالى لقطاعات الأعمال المختلفة، وأهم ما يحتاج إليه هذا النوع من المعلومات أن تكون المعلومة سليمة وكاملة وموثوقاً فى صحتها.

- معلومات المهنة أو سر الصنعة، فكثير من المشروعات يتوقف نجاحها على مثل هذا السر، ولقد جعل المشرع الأمريكى من التلاعب بمثل هذا النوع من المعلومات جريمة فيدرالية.

- ومن المعلومات المهمة أيضاً تلك المتعلقة بخطوات الانتاج، فالسلعة أو الخدمة تمر بعدد كبير من المراحل حتى تصل إلى مرحلتها النهائية. وتعد هذه المراحل من المعلومات المهمة التى يحرص أصحاب الأعمال على حفظها، وحمايتها من الاطلاع عليها من قبل الغير.

- تحتفظ قطاعات الأعمال المختلفة بنوع آخر من المعلومات ذات الطابع الشخصى، والتى تتمثل فى جميع البيانات الشخصية المتعلقة بالعاملين بها. ولا شك فى أهمية حماية هذه المعلومات.

- وهناك كذلك المعلومات التى تتخذ شكل منتجات كالكتب وبرامج الحاسب

الآلى، والأعمال الأدبية والموسيقية والخرائط والإعلانات وغير ذلك من المعلومات التى تتخذ شكل المنتج، وتقوم قوانين الملكية الفكرية بحماية هذا النوع من المعلومات.

– المعاملات اليومية كالخطابات والمذكرات ومسودات التقارير والمحادثات وغيرها، تشكل معلومات على جانب كبير من الأهمية لنشاط المؤسسة، وهو ما يتطلب حمياتها من الوصول إليها والتلاعب بها.

– وأخيراً، فإن هذه الأنواع المختلفة من المعلومات تقتضى توفير الإجراءات الأمنية واللازمة لحمايتها، وتعد هذه الإجراءات الأمنية من ناحية أخرى من المعلومات المهمة بالنسبة إلى المؤسسة والتى يتعين أيضاً حمايتها (١).

• **النقود في عالم الحاسبات الآلية:**

أصبح الآن لبعض المعلومات، وخاصة بعد الدخول فى عصر الحاسبات الآلية، قيمة نقدية(*). وتدل المؤشرات على تنامى عدد الجرائم المنصبة على هذا النوع من المعلومات لذا بدأت تتضافر الجهود لتوفير أكبر قدر من الحماية لها.

ولقد أصبح التعامل النقدى فى الوقت الراهن يتم بصورة كبيرة عبر الحاسبات الآلية، بحيث أصبح استخدام اصطلاح النقود الالكترونية يتزايد مقارنة بمصطلح النقود العادية، وأصبح من المألوف أن تبرم صفقات كاملة عن طريق شبكة الإنترنت يتم على أساسها تبادل السلع أو الخدمات إلكترونياً، والوفاء بقيمتها

(1) Parker (Donn), Op. cit., pp. 34 - 38.

(*) والواقع أنه يمكن القول أننا بصدد الدخول فى الثورة النقدية الثالثة، فقد كانت الثورة الأولى منذ حوالى ٢٥٠٠ عاماً عندما بدأ التعامل بالعملة المعدنية، ثم بدأت الثورة الثانية فى القرن الخامس عشر عندما بدأ ظهور العملة الورقية والتعامل بها بجانب العملة المعدنية. أما الثورة الثالثة والتى نشهد بدايتها الآن تهدف إلى تحويل التعامل إلى نوع جديد من النقود ألا وهى النقود الإلكترونية والنقود البلاستيكية (البطاقات الإئتمانية). ولا يعنى ذلك حلول النقود الإلكترونية والبلاستيكية واندثار النقود المعدنية أو الورقية. فلا تزال هذه النقود محل تداول فى العالم كله، إلا أن النمو المستمر للنقود الإلكترونية وزيادة الثقة والتعامل بها، سوف يجعل سيادة هذا النوع من النقود مستقبلاً أمراً محتوماً بلا شك.

عن طريق النقود الالكترونية. ويعني الوفاء بالنقود الإلكترونية اجراء عملية مقاصة بين حسابين يمتلكهما طرفي المعاملة، ويترتب على هذه العملية اقتطاع قيمة العملية من حساب المدين واضافتها إلى حساب الدائن دون أن يحدث أي تبادل مادي أو ملموس للنقود.

**٢- الصورة التي توجد عليها المعلومات:**

أشرنا فيما سبق لأنواع المعلومات المختلفة، والتي تشكل المحل في جرائم المعلوماتية. ولا يقتصر الاختلاف على نوع المعلومة وإنما يمتد أيضاً إلى الصورة التي توجد عليها. فالمعلومة قد تكون مشفرة أو غير مشفرة، كما أنها قد تكون مقروءة أو مسموعة. وتتوقف قيمة المعلومة والحماية اللازمة لها في كثير من الأحيان على الصورة التي توجد عليها، فتغيير حرف على سبيل المثال في معلومة مشفرة يختلف اختلافاً كبيراً عنه في معلومة غير مشفرة. فالتغيير في الحالة الأولى يؤدي إلى تدمير لمعنى هذه المعلومات، إلا أنه لا يؤدي بالضرورة إلى تلك النتيجة في الحالة الثانية إذ قد يقتصر الأمر على مجرد الانتقاص من صحتها.

وقد تتغير الصورة التي توجد عليها المعلومة بسبب التلاعب بها بحيث تظل المعلومة موجودة ولكن بدون معنى أو فائدة، فبإدخال أحد البرامج الخبيثة (الفيروسات) إلى الحاسب الآلي من شأنه أن يغير من صورة المعلومة على نحو سلبي، ويؤدي إلى تحويل المعلومة على الشاشة إلى مجموعة من الحروف المبعثرة، التي تتهاوى بسرعة كبيرة إلى القاع مكونة كومة كبيرة من الحروف(*).

**٣- الشكل:**

يتعلق الشكل بصفة عامة بالطريقة التي تكتب بها المعلومات. وفي مجال

(*) وعلى الرغم من أن المعلومة مازالت موجود على الشاسة، إلا أنها قد فقدت كل أهمية لها، ما لم يمكن اعادتها إلى صورتها الأولى بالاستعانة بنسخة إضافية يُحتفظ بها كضمان في حالة فقد أو تدمير الأصل. كما قد يقوم الفيروس أيضاً بتغير صورة المعلومات في ذاكرة الحاسب وذلك بتغير ملف البيانات الذي يحتوي على المعلومات في ذاكرة الحا سب، وتحويلها إلى خليط من الحروف.

المعلوماتية أو تكنولوجيا المعلومات يقصد بالشكل أيضاً الطريقة التى تكتب بها المعلومات من خلال الحاسبات الآلية(*).

**٤- وسائط تخزين المعلومات:**

تتطلب المعلومة، بطبيعتها، وجود وسط تخزن فيه حتى لو كان هذا الوسط هو مجرد العقل البشرى. وتختلف وسائط تخزين المعلومات فقد تكون أحباراً أو ألواناً، وينطبق ذلك على جميع المعلومات المدونة فى أوراق "Hard-Copy documents"، أو قطع ووصل الكترونى كالإشارات الرقمية فى الحاسبات الآلية "Electronic switches"، ولا شك أن التلاعب الذى قد يقع على هذا الوسط من شأنه أيضاً تعريض المعلومات للخطر.

---

(*) ويتضمن الشكل:

- أسلوب المبرمج فى كتابة البرنامج "Style" مثل أساليب التركيب ومصطلحات التسمية وأنواع التعليق والشرح وغيرها.
- الحروف التى تتعلق بالطباعة.
- "Font" اللغة البرمجية "Language" وهى مجموعة الرموز والكلمات والقواعد المستخدمة لكتابة برنامج الحاسب الآلى.
- القواعد اللغوية "syntax" وهى القواعد التى تتعلق بترتيب الكلمات والعناصر المكونة للتعليمات فى لغات البرمجة.
- قواعد التشفير "Encoding" وهى مجموعة من القواعد الواضحة التى تحدد طريقة تمثيل المعلومات بالشفرة، بحيث يمكن فك هذه الشفرة فيما بعد لقراءة محتوى هذه المعلومات.
- الهيئة أو شكل الطباعة أو النسق "Format" وهى القواعد المتعلقة بتنظيم البيانات فى صفوف أو أعمدة أو عناوين... إلخ.
- حجم الذاكرة أو حجم الملف أو المستند "Size".

ومن الأهمية أن يمتد نطاق الحماية إلى القواعد المتصلة بالشكل وذلك لمنع التلاعب بالمعلومات عن طريق المساس بهذه القواعد. فتغيير شكل المعلومة قد يترتب عليه تغيير فى معناها، أو فقدانها تماماً. ويتأتى الاتلاف المتعمد فى هذه الحالة عن طريق تغير الشكل إلى شكل آخر لا قيمة له. ومن المشكلات التى ظهرت مؤخراً والتى تتعلق أيضاً بالشكل ما يطلق عليه بمشكلة الألفية الثالثة، فنتيجة لخطأ فى الشكل الذى تمت به كتابة التاريخ الميلادى فى أكثر برامج الحاسب الآلى أدى إلى عجز هذه البرامج عن تحويل التاريخ عند نهاية عام ١٩٩٩ إلى عام ٢٠٠٠ وإنما تحول إلى ١٩٠٠، مما ترتب عليه ظهور بعض المشكلات العملية.

ب- الخصائص التكميلية للمعلوماتية:

تناولنا فيما تقدم السمات أو الخصائص الأساسية للمعلومات، ومع ذلك قد نستعين ببعض الخصائص التكميلية لتساعدنا على الوقوف على طبيعة المعلومة، وبالتالى التعرف على نوع الحماية اللازمة لها، ويمكن تلخيص هذه الخصائص فيما يأتى:

* مدى إتاحة المعلومة "Availability"، فقد يكون الوصول إليها وتحصيلها بصفة عامة سهلاً وميسوراً للجميع أو مشروطاً، فهل تسمح طبيعتها بأن تكون معلومة للجميع أم أنه يجب حصر العلم بها فى مجموعة من الأفراد دون سواهم.
* أهمية المعلومة وقيمتها ومقدار ما تعطيه من فائدة "Utility".
* مقدار ما تتمتع به المعلومة من الصحة "Integrity"، والمصداقية "Authenticity".
* حيازة المعلومة، وذلك بتحديد مالكها وحائزها أو من يسيطر عليها "Possession".
* المعلومة من حيث الكم، ويتوقف ذلك على تحديد حجم المعلومامة كعدد أجزائها أو عدد الحروف والكلمات والصفحات التى تتكون منها "Quantity".
* المكان الذى توجد به المعلومة "Locations".
* قيمة المعلومة من حيث الزمان، وذلك من خلال الوقوف على ما إذا كان للمعلومة قيمة فى وقت معين وهل تتناقص هذه القيمة أو تنتهى بانتهاء هذا الوقت "timeliness".
* موضوع المعلومة، عن طريق تحديد الموضوع أو العنوان الذى تندرج تحته المعلومة "Subject".
* الأثر الذى تتمتع به المعلومة، ويتوقف ذلك على تحديد التأثير الذى يحدثه معرفة المعلومة أو حيازتها أو استعمالها "Subject".
* الوسائل التى يتم اتخاذها لحماية المعلومة "Security and Legal Protection".

## الفرع الثاني

## المعلوماتية ومرحلة ما بعد الحداثة

كثرت النعوت والأوصاف التى أضفاها العلماء والمفكرون على المرحلة الحالية التى يمر بها المجتمع الإنسانى منذ اصطدامه بما يسمى بالموجة الثالثة Third Wave فى التطور(*)، كما يقول المفكر الأمريكى «ألفين توفلر»(1)، فمنهم

---

(*) وذلك على أساس أن الموجة الأولى هى معرفة الإنسان للزراعة، والموجة الثانية هى الثورة الصناعية، والموجة الثالثة هى مرحلة ما بعد الثورة الصناعية أو ما بعد التصنيع. ويطلق عليها ألفين توفلر مرحلة المجتمع المعلوماتى. ويوضح ذلك العالم الاجتماعى الشهير دانيل بل Daniel Bell فى مؤلفه: (قدوم مجتمع ما عبد الصناعى.. The Coming of Post - in-dustrial society).. بقوله: «إن تكنولوجيا المعلومات هى وقود الثورة الصناعية الثالثة، وأن المعلومات فى حد ذاتها تعد هى المادة الخام الأساسية للإنتاج، والتى يعتمد المجتمع على إنتاجها وإيجادها والاستفادة منها.

وأن كل أولئك قد احدث تحولاً جذرياً فى مفهوم العمالة الصناعية القديمة التى تعين عليها أن تنسحب لتفسح المكان لوافد جديد يتمثل فى العمالة التى يكون بمقدورها التعامل مع صناعة المعلومات، وبالتالى أصبح التهافت على من يجيد فن التعامل مع التقنيات المستخدمة فى صناعة المعرفة وإدارتها، وكذلك الذين يقومون بعملية تنظير هذه المعرفة». للمزيد يراجع مؤلفه:

- BELL (Daniel): "The Coming of Post - Industrial Society, Aventure in Social Forcasting" Basic Books, New York, 1973.

وجدير بالذكر أن تسمية مرحلة المجتمع المعلوماتى التى أطلقها آلفين توفلر هى التسمية التى أخذت بها توصية لجنة وزراء الدول الأعضاء فى المجلس الأوروبى بخصوص مشاكل قانون الاجراءات الجنائية المتعلقة بتكنولوجيا المعلومات فى ١١ سبتمبر سنة ١٩٩٥، حيث ورد فى صدر هذه التوصية: ... إن التطور فى نظم المعلومات الإلكترونية سوف يعجل بتحول المجتمع التقليدى إلى مجتمع معلوماتى من خلال ايجاد فضاء جديد لكل أنواع الاتصالات والعلاقات.

"The Development Etectronic Information Systems Will Speed up Transformation of Traditional Society Into an Information Society by a New Space For all Types of Communications and Relations".

(1) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والاجرائية لجرائم المعلوماتية – مرجع سابق – ص ١١.

من يصف هذه المرحلة بمرحلة ما بعد الصناعة، أو ما بعد التصنيع، أو ما بعد الحداثة، أو مرحلة ما بعد التحديث، أو ما بعد المعاصرة أو ما بعد العصرية، أو ما بعد المادية التاريخية(*).

وكل هذه النعوت والأوصاف إنما تعبر عن مدى ضخامة القفزات العلمية الهائلة التى تحققت فى شتى مناحى الحياة، ومدى تنوع الانجازات التى طرحت ثمارها فى هذه الآونة الأخيرة. والواقع أن العصر الذى نعيش فيه يمتد ليشمل كل هذه التطورات والإنجازات بسمتها وسماتها. ومن هذا المنظور يرى الكثير من المفكرين الغربيين(١) أن التعبير الذى يمكن أن تندرج تحته كل هذه الانجازات والتطورات بمسمياتها المختلفة هو مصطلح ما بعد الحداثة Postmoderne/Post - Modernity(٢).

(*) ومن الصفات الأخرى ما بعد الشمولية، أو ما بعد الرأسمالية، ونظائرها من منظومة الـ (ما بعديات). كما أن منهم من يطلق على هذا العصر.. عصر ثورة المعلومات والاتصالات أو عصر المعلوماتية، أو عصر السماوات المفتوحة، أو عصر التكنولوجيا الرقمية، أو عصر الانترنت، أو عصر الثورات التكنولوجيا المتقدمة.

(١) من أبرز هؤلاء المفكر الفرنسى الشهير جان فرانسوا ليوتار. راجع مؤلفه:

- LYOTARD (Jean - Francois): "La Condition Postmoderne", Editionsde Minuit, Paris, Septembre, 1979.

والترجمة العربية لذات المؤلف:

جان فرانسوا ليوتار – (الوضع ما بعد الحداثة – ترجمة أحمد حسان – دار شرقيات – القاهرة – سنة ١٩٩٤.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢.

- ونظراً لأن مذهب ما بعد الحداثة هو الأكثر انتشاراً فى الثقافة الغربية. وهو الذى تنصهر فى بوتقته سائر مظاهر الإنجاز والاعجاز – ومنها المعلوماتية Informatique Informative التى تعنى (فى أبسط عبارة لها) أن يصبح كل سكان العالم فى حالة معرفة فورية بما يحدث لديهم ولدى الآخرين، وأن يكون مقدور كل منهم التأثير فى الآخرين والتأثر بهم – فسوف نتعرض فى عجالة لأهم جوانب هذا المذهب، حيث أنه لا مراء فى أن الجرائم التى واكبت التقدم المذهل فى تكنولوجيا المعلومات والاتصالات لم تأت من فراغ، بل كانت نتيجة شيوع ثقافة معينة تدعو إلى التمرد بكافة صوره ضد مختلف المؤسسات السياسية والاقتصادية

-/-

--- والاجتماعية والدينية، وخلخلة ما هو ثابت وراسخ فى شتى مناحى الحياة العلمية والعملية، حتى لو تم ذلك - لدى غلاة ومتطرفى ما بعد الحداثة - بطرق غير مشروعة إذا قيست هذه الأعمال بمقاييس القوانين العقابية. وبالتالى يمكن اتخاذ هذه الثقافة المتمردة متكأ لتفسير هذه النوعية من الجرائم.

والبداية في هذا الشأن الوقوف على المعنى اللغوى لمصطلح ما بعد الحداثة Postmodernity .Postmoderne

وتجدر الإشارة هنا أنه من الملاحظ أن هناك بعضاً من الباحثين يستخدمون مصطلحى Post-modernity و Postmodermisn كمترادفين. فى حين يرى البعض الآخر أن المصطلح الأول أكثر التصاقاً بثقافة ما بعد الحداثة فى حالة السكون أو الوصف الوجودى لها، أما المصطلح الثانى فيعبر عن الحركة أو الديناميكية أو التفاعل لهذه الثقافة. بعبارة أخرى: أن مصطلح Postmodernity - يهدف إلى دراسة الجانب الاستاتيكى لثقافة ما بعد الحداثة. أما المصطلح Postmodenism - فيهدف إلى دراسة الجانب الديناميكى لها. يراجع على سبيل المثال-

- Adams (Daniel J.): "Toward a theolagical Understanding of Polst-mernism", availabbe at: h Th: // www. yohoo. com

وعودة للمعنى اللغوى.. حيث نجد أنه قد ورد فى Dictionary. com أن تعتبر ما بعد الحداثة - أو ما بعد الحديث - تعتبر يتصل بالفن أو العمارة أو الآدب الذى يتمرد (reacts - against) على المبادئ الحديثة السابقة من خلال إعادة إدخال العناصر التقليدية أو الكلاسيكية أو من خلال استخدام الأساليب أو الممارسات الحديثة بشكل متطرف To extremes. كما ورد فى Word Net أن تعبير ما بعد الحداثة نوع من الفن والأدب وخاصة العمارة متمرد In reac-tion against على القواعد والممارسات التى رسمتها المعاصرة أو الحداثة.

وإذا تجاوزنا المعاجم اللغوية واتجهنا شطر المراجع العلمية التى تناولت ذات الموضوع، ذكر استاذنا الدكتور/ هلالى عبد اللاه أننا نجد حواراً مازال مستعراً ودخاناً ما فتئ داخنا حول تحديد ماهية مصطلح ما بعد الحداثة، ويعزى ذلك إلى تشعب الآراء حوله، وتجاوز الحدود بين مختلف فروع المعرفة فى التعامل معه، وسعى أطراف عديدة للاستشهاد به واستخدامه للتعبير عن اهتمامات وتوجيهات متباينة.

وإذا كانت هذه المراجع والمؤلفات قد عجزت عن إعطاء تعريف دقيق لهذا المصطلح، إلا أن الكثير منها يكاد يتفق على أن (ما بعد الحداثة) حركة تمرد - كما أشارت المعاجم اللغوية - ضد كافة المؤسسات السياسية والاقتصادية والاجتماعية والدينية، وخلخلة كل ما هو ثابت وراسخ فى شتى مناحى الحياة العلمية والعملية.

فلقد شملت نظرة الشك والارتياب لدى أنصار حركة ما بعد الحداثة كافة المؤسسات المجتمعية وعلى رأسها الدولة باعتبارها أداة للهيمنة والاستبداد. يراجع:

- Foucault (Michel): "La Volonté de savoir - Histoire de La sexualité", Gallimard, Paris, 1976, pp. 52 - 53.

-/-

--- مشار إليه لدى دكتور/ محمد حافظ دياب: (خطاب ما بعد الحداثة: انحلال الحتمى وإغداء المختلف) متاح في:.hTTp: // www. rezgar. com / debat / show. art -

- حيث أن المفكر الفرنسى من أصحاب هذه النظرة الذى ركز على تحليل السلطة، وتبيان خطأ ومحدودية فهمها بحصرها فى كيان محدد هو جهاز الدولة المركزى.

راجع بتوسع فى ذات المعنى: د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٦ وما بعدها. وفى جانب آخر... فقد تميزت مرحلة ما بعد الحداثة بتزايد الاهتمام بالآثار المدمرة للعلم التطبيقى من جراء جشع الرأسمالية وآثار ذلك على البيئة. ذلك أن التحديث الانعكاسى – أى التدمير والدمار الطائش وغير المقصود – الذى يسببه التحديث أوجد ما أسماه بيك Beck (مجتمع المخاطر)، أو ما أشار إليه ستانفورد جيدنز Stanford Giddens بمصطلح (عدم اليقين المصنوع Manufactured Uncertainty)، فارتفاع درجة حرارة الأرض وتلوث واستنزاف أجزاء البيئة والمخاطر المرتبطة بالإنتاج الضخم من الدواجن والحيوانات من أجل الغذاء (مثل المناعة ضد بعض المضادات الحيوية)، وتكاثر الأسلحة النووية والكيماوية وغيرها من أسلحة الدمار الشامل، كل هذه أمثلة على التبعات الخطيرة غير المقصودة للحداثة... وفى رأيهما أن من الضرورى الالتفات إلى ورطة الخاسرين فى مجتمع الحداثة المتأخرة فى الغرب وعلى مستوى العالم.. ولا تشمل فئة الخاسرين فى مرحلة المتأخرة أولئك الذين أفقدتهم التنمية وظلمتهم فحسب، بل وتضم أيضاً شعوب العالم الغنى. راجع: (قراءات معاصرة فى نظرية علم الاجتماع – ترجمة مصطفى خلف عبد الجواد – مطبوعات مركز البحوث والدراسات الاجتماعية – كلية الآداب – جامعة القاهرة – سنة ٢٠٠٢ – ص ١٢٥).

وعلى الجانب الاجتماعى وصل الشك إلى الأسرة، حيث وضعت علامة استفهام كبيرة حول جدوى النظام الأسرى كضرورة اجتماعية أو أخلاقية، إذ لم يعد من الضرورى – فى تقدير اتجاه ما بعد الحداثة – الحرص على التماسك الأسرى أو تنشئة الطفل داخل أسرة متماسكة.

وعلى الجانب الدينى وضعت نفس علامة الاستفهام. فإذا كانت الحداثة تنظر إلى الدين على أنه أمر غير علمى، حيث أنه قائم على افتراض وجود كائنات غيبية أو ميتافيزيقية، لا تدخل تحت ما يمكن التحقق منه بالحواس وإدخاله تحت نطاق التجربة، فصار فى حس الحداثيين أن الدين خرافة، بمعنى أنه مناقض للعلم، وإن كان بعضهم يرى أنه لا بأس أن يتخذ الإنسان تلك الخرافة دينا له ويؤمن بها.

أما مذهب ما بعد الحداثة فيرى صحة جميع الأديان، لا من حيث أنه يعترف بالوحى أو بوجود الله، بل من حيث إنها جميعاً بنى ثقافة، ولا أحد يملك أن يحكم عليها بأنها خطأ، إذ ليس لدى أحد معيار مطلق يمكن أن يقاس به الدين الحق من الباطل.

لذلك لا تحارب حركة ما بعد الحداثة الأديان، بل تشجعها وتدعو للتعايش بينها، يستوى فى ذلك الأديان السماوية وغير السماوية. وقد يبدو من ذلك أن نظرة ما بعد الحداثة إلى الدين نظرة حيادية. ولكنها عند التمعن يتضح أنها نظرة إلحادية، ويتأكد هذا الإلحاد بالاضافة إلى أن

**أولاً: ملامح مرحلة ما بعد الحداثة:**

وإذا كانت مرحلة ما بعد الحداثة قد حملت حركة التمرد والخروج على الثوابت فى مجلات الأدب والفن والعمارة، فإنها سرعان ما أمتدت إلى مجالات أخرى. ينصب اهتمامنا ودراستنا بشأنها على مجال تكنولوچيا الاتصالات والمعلومات. حيث اكتست حركة التمرد فى هذا المجال ثوب التحدى والمواجهة، حتى تعدى ذلك الكيانات الفردية واصلاً إلى مستويات أعلى ومستهدفاً الدولة ومؤسساتها الحيوية. ومن أمثلة هذا التمرد ويمثله من اعتداء الأمثلة التالية:

- قيام بعض القراصنة Hackers المتواجدين على الأراضى الروسية، باختراق نظم حاسبات حكومية فى الولايات المتحدة لمدة عام كامل، حيث قاموا بسرقة «معلومات غير سرية ولكنها حساسة» من أجهزة حاسبات عسكرية.

The intruders stole "Unclassified but still sensitive information us military computers"(1).

- أغار القراصنة على شبكات غير سرية فى وكالة الفضاء الأمريكية NASA، ومواقع أسلحة ذرية Nuclear Weapons(*).

---

— هذه الحركة تساوى بين الأديان السماوية التى من صنع الإنسان، إنها تطرح الثقة فى كافة المؤسسات الدينية وتجردها من مصداقيتها، وترى عدم الجدوى من اللجوء إليها. (د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ص ١٨ ، ١٩).

(1) "World: Americas Russian hackers attacked Pentagon: BBC news, October 8 1999, available at: http: // news, bbc. co. uk / 1 / hi / World / americas / 469006. stm.

(*) وأيضا من جرائم الاختراق.. قيام قرصان بريطانى U. K. Hacker باختراق ما يقرب من مائة حاسب تتعلق بالحكومة والقطاع الخاص مما تسبب فى عرقلة عمليات عسكرية Disrupting military operations فى قاعدة بحرية فى ولاية نيوجيرسى at a Navy station in New Jersey وخسارة مقدارها ٩٠٠,٠٠٠ دولار.

راجع فى ذلك:

- "U.S. Cbarges U.K. Hacker did $ 900.000 in domage", Yahoo, News, available at.../ story, news. yahoo. com/news? tmpl = story & u = / nu / 2002 1113/wL- nm/ tech - hacker - de.

=/=

وكان من جراء ذلك قيام البنتاجون The pentagon بإنشاء مركز الحرب المعلوماتية "a cyber - war centre" للدفاع عن الولايات المتحدة الأمريكية ضد القراصنة وتحديد وسائل الهجوم على شبكات حاسب الأعداء(1).

- اختراق نظم الحاسب الآلي للمنتدى الاقتصادى العالمى فى دافوس بسويسرا، وسرقة معلومات سرية تتعلق بعدد من الشخصيات الثرية المؤثرة التى شاركت فى المؤتمر وإرسالها إلى إحدى الصحف السويسرية(*).
- اختراق موقع رئاسة الجمهورية البلغارية على شبكة الإنترنت، فقد أعلنت المتحدثة باسم الرئاسة البلغارية أن السلطات فى العاصمة صوفيا شددت

---

-- قيام طالب أمريكى يدعى دينيس موران يبلغ من العمر ١٨ سنة باختراق موقع شرطة لوس أنجلوس Los Angeles الخاص بمكافحة المخدرات على الإنترنت بغية إيقافه وتخريبه (http: .// 100. 8k. com / 25. htm).

نجاح قراصنة الحاسب فى ٤ مايو ٢٠٠١ فى اقتحام أحد مواقع البيت الأبيض الأمريكى وتعذر الوصول إلى الموقع لمدة ساعتين كاملتين (http: // www. aljazcera. net/ science - tcch/ 2001/ 5/5 - 27 - 1. htm)

بل لقد نجح هؤلاء القراصنة فى اقتحام موقع «الاستجابة الكمبيوترية الطارئة سيرت» على شبكة الإنترنت والذى يتولى حراسة الشبكات الإلكترونية وتوفير الحماية لها من اختراقات الفضوليين وقراصنة المعلومات وتمكن المهاجمون من تعطيل الموقع الذى يقوم بتحذير الوكالات الحكومية من تلقى خدمات الموقع التابع لإحدى الجامعات الأمريكية من الوصول إليه، وذلك عبر بث كميات هائلة من المعلومات سدت طرق الوصول إليه. وقال أحد المسئولين عن الموقع «نحن نهاجم كل يوم، وكان هذا واحداً من الهجمات التى نتعرض لها، ولكن الدرس الذى يجب أن نتعلمه أنه لا يوجد موقع حصين على شبكة الإنترنت ضد هذا النوع من الهجمات التى تتسبب فى مشاكل تشغيلية وهى تحتاج إلى وقت لإصلاحها، (http: // www. aljazeera. net/ science tech/ 2001/ 5/5 - 27 - 1 - htm)

(1) "World : Americas Russian hackers attacked pentagon", op. cit.

(*) وتتضمن هذه البيانات تفاصيل بطاقات الائتمان وأرقام الهواتف المحمولة والعناوين الخاصة بهذه الشخصيات. راجع:

- «قراصنة الكمبيوتر يتسللون لمنتدى دافوس». بى بى سى أون لاين متاح فى: http: // news. bbc. co. uk/ hi/ arabic/ news/ newsid 1153000/ 1153124: stm

مشار إليه لدى: د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٢٢.

الإجراءات الأمنية فى أعقاب دخول أحد قراصنة الإنترنت لموقع رئاسة الجمهورية الرسمى على شبكة الإنترنت وقيامه بمحو كل محتوياته. وكان دافعه من وراء هذا العمل هو التعبير عن السخط من الحالة المزرية لحياة والديه، والبطالة التى يعانى منها، وهجرة أصدقائه للخارج لتحسين مستقبلهم(١).

وفى حادث مماثل دخل بعض قراصنة الإنترنت إلى موقع حزب رئيس الدولة البلغارية،وتركوا له رسالة بذيئة(٢).

وبالإضافة إلى هذه الأمثلة ونظائرها كثير، اتخذ التمرد والخروج على قواعد الرقابة على شبكة الإنترنت شكلاً آخر، عندما كشف بعض أشهر قراصنة الحاسب فى العالم النقاب عن خطة لتوفير برامج كمبيوتر مجانية للتصفح المجهول عبر الإنترنت فى البلدان التى تفرض رقابة على الشبكة. وأذاعت مجموعة المتسللين التى تطلق على نفسها تسمية «هاكتى فيسمو» برنامجاً يسمح لمستخدمى الإنترنت بإخفاء رسائل داخل صور موضوعة على الإنترنت والالتفاف حول أشهر أساليب الشرطة فى الرقابة.

وتستعد المجموعة قريباً لإطلاق تكنولوجيا – لو استخدمت على نطاق واسع – فسوف تسمح لأى شخص بإقامة شبكات مجهولة الهوية يمكن لمتصفحى الإنترنت الوصول إليها وتقاسم المعلومات دون أن يتركوا أى أثر(*).

---

(1) - http; // www. aljazeera. net/ news/ europe/ 2001/ 1/1 - 19 - 8. htm.

(٢) الموقع نفسه.

(*) وقد جاء إعلان المجموعة وهو نتاج مشروع استمر عامين شارك فيه كبار قراصنة الكمبيوتر فى العالم من خلال مؤتمر H2, H2 الذى عقد فى شهر يوليو سنة ٢٠٠٢ فى New York واستمر لمدة ثلاثة أيام. ويسمح برنامج ميكستر – والذى يعرف فنيا باسم البروتوكول – لمستخدمى أجهزة الحاسب العادين بإنشاء نسخة غير مركزية من الشبكات التى تستخدمها الحكومات وكثير من الشركات فى إقامة شبكات آمنة معزولة عن الشبكة العامة للإنترنت. وبرنامج المجموعة مصمم بحيث يتفادى البرامج الواقية ضد القرصنة التى لا تسمح سوى
=/=

كذلك كان من جراء تأثير ثقافة ما بعد الحداثة والتمرد على ما هو قائم وراسخ والخروج على ما هو مألوف وتقلدى، انتشار المواقع الإباحية على شبكة الإنترنت، والتى ما فتئت تبث بالصوت والصورة كل ما يرغب الفتى أو الفتاة فى الابتعاد عن التفكير فى تكوين أسرة. والاستعاضة عنها بفكرة الصحبة وما شابها حيث الإشباع الجنسى والعاطفى، دون تحمل لمسئوليات الزواج(1) وأعبائه الجسام(*). هذا بالإضافة إلى المواد الإباحية الطفولية كما سنرى فيما بعد.

ويضاف إلى ما سبق تلك المجموعات التى تطلق على نفسها «مجموعات الكراهية على الإنترنت Hate groups on the Internet» تلك المجموعات التى تزدرى بكل القيم الدينية والأخلاقية والاجتماعية السائدة فى المجتمعات وبصفة خاصة تلك المرتبطة بالإسرة(2). كذلك مواقع الإلحاد التى تطالب بإلغاء الدين، والدولة والأسرة وتحرير الإنسان من تلك الأصفاد والقيود(3).

لهذه الأسباب مجتمعة لم يكن غريباً أن يصف المفكر الإنجليزى الشهير

---

-- بدخول جزئى لشبكات الحاسب العالمية، والتى تحول دون الوصول إلى أنواع معينة من العناوين المخطورة على الشبكات الداخلية للشركات وإلى الدول التى تفرض قيوداً على الدخول إلى شبكة الإنترنت.

– راجع: «قراصنة الكمبيوتر يتحدون الرقابة على الإنترنت» عالم الكمبيوتر والإنترنت – سبتمبر ٢٠٠٢ – موقع مصراوى Masrawy متاح فى:

- http: // www. alamal/ computer. com/

(1) - http: // www. craving porn., com/

- htt: // chatropolis. com/

- http; // www. streamchat. com/

(*) الأمر الذى ساهم – مع بعض العوامل الأخرى – فى انتشار ظاهرة العنوسة سواء على مستوى العالم ككل أم على مستوى البلاد العربية والإسلامية. حول مخاطر العنوسة على المرأة والأسرة والمجتمع راجع بصفة خاصة:

الشيخ شمس الدين: «العوانس صرخة فى وجه المجتمع والقانون» – القاهرة – مركز الراية للنشر والإعلام – الطبعة الأولى – سنة ٢٠٠٢.

(2) http; // www. bepl. net/ - rfrankli/ hatedir. htm.

(3) http; // www. wichvox. com/ cases/ religioushate. htm.

أنتونى جيدنز Anthony Giddens(*) العالم الذى نعيش فيه بأنه «عالم منفلت Runaway World» لا يمكن الإمساك بتلابيبه أو إخضاعه للسيطرة، وأن يصدر كتاباً يحمل هذه التسمية(١).

وربما يكون هذا الانفلات الذى شمل شتى مناحى الحياة، بما فيها الانفلات الدينى والأخلاقى والاجتماعى والاقتصادى والسياسى، قد يعطى تفسيراً مقنعاً لما نراه اليوم من النمو المتزايد والمطرد للجرائم الكونية أو المعلوماتية والتى من أجلها حرص مجلس أوروبا على صياغة هذه الاتفاقية – أى اتفاقية بودابست – لمكافحتها والتغلب عليها(٢). كما حرصت بعض الدول على أن تضمن تشريعاتها هذه النوعية من الجرائم إما عن طريق النص عليها استقلالاً فى تشريعات مستقلة(٣)، وإما عن طريق تحديث قوانيها وإدماجها فى هذه القوانين(**).

---

(*) هو أستاذ علم الاجتماع بجامعة كمبردج، وهو يعد من أشهر علماء هذا التخصص الذين ذاعت شهرتهم لا لكثرة مؤلفاتهم فقط ولكن لما يقدمونه من إسهامات نظرية ومنهجية. كتب ما يربو على مائتى مقال ما بين مقال بحثى أو مراجعة كتب أو مقال صحفى. أما قائمة الكتب التى كتبها فتضم ستة وثلاثين كتاباً من بينها كتاب «علم منفلت: كيف تشكل العولمة حياتنا» سنة ١٩٩٩ والذى ترجم إلى العربية. للمزيد عن السيرة الذاتية لهذا المفكر راجع:

– أنتونى جيدنز: مقدمة نقدية فى علم الاجتماع ترجمة د. أحمد زايد وآخرين – مطبوعات مركز البحوث والدراسات الاجتماعية – كلية الآداب – جامعة القاهرة – ٢٠٠٢ – ص ص ٧، ١٢.

(1) Giddens (Anthony): "Runaway world: How Glbalization is reshaping our Lives". London. Profile books. 1999.

وقد ترجم هذا الكتاب إلى العربية:

– أنتونى جيدنز: «عالم منفلت: كيف تعيد العولمة صياغة حياتنا؟» ترجمة د. محمد محيى الدين، ميريت للنشر والمعلومات، القاهرة، ٢٠٠٠.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٢٥.

(٣) ومثال ذلك قانون إساءة استخدام الحاسب فى المملكة المتحدة الصادر فى ٢٩ يونيو سنة ١٩٩٠، والذى طبق اعتباراً من ٢٩ أغسطس سنة ١٩٩١.

(**) ومن أبرز هذه النوعية من التشريعات قانون العقوبات الفرنسى الجديد الصادر سنة ١٩٩٢ والمعمول به منذ أول مارس سنة ١٩٩٤ والذى أضاف فصلاً ثالثاً للباب الثانى من القسم الثالث من قانون العقوبات تحت عنوان: «انتهاكات نظم المعالجة الآلية للبيانات Des atteintes aux systems de traitement automatisé de données

ويتكون هذا الفصل من المواد ٣٢٣/١ إلى ٣٢٣/٧.

ثانياً: الشراكة العالمية في عصر المعلوماتية:

أيا ما كان الجانب المظلم من مذهب ما بعد الحداثة، وما يمثله من انفلات وتمرد واستعلاء، فإنه فى جانبه المضئ لدى من يقولون به يعكس واقعاً جديداً يدعو إلى الإنساق الفكرية المفتوحة(*) التى تفتح الباب لمشاركات إنسانية أوسع وأرحب من خلال فكرة العولمة(**) Mondialis-ation / Globalization من حيث هى مبدأ، أى الشراكة العالمية فى مناحى الحياة المختلفة مع اقتسام المغانم والمغارم، ومضمون لجوانب الحياة المختلفة السياسية والاقتصادية والثقافية والتقنية، ووسيلة لربط أجزاء العالم المختلفة بعضها ببعض عن طريق شبكة الانترنت والشبكات المعلوماتية المتصلة بها. بيد أن هذا الجانب المضئ من مذهب ما بعد الحداثة سرعان ما تناوشه الظلمة، وذلك على أساس أنه إذا كانت شبكة الإنترنت والشبكات المعلوماتية المتصله بها قد أصبحت التعبير الأمثل عن ثقافة ما بعد الحداثة، وشرايين الربط والاتصال بين مختلف بقاع العالم. غير أن هذه الايجابيات يقابلها الكثير من السلبيات التى تتمثل فى الاستخدام غير المشروع لهذه الشبكات، كما تمت الأشارة سلفاً(١).

ونظراً لتشعب تأثير العولمة وقد أمست تفرض أنظمتها ومفاهيمها وفكرها على الجميع أفقياً على النطاق الدولى والوطنى، ورأسياً فى الجوانب الاقتصادية والسياسية والاجتماعية والثقافية والمعلوماتية للمجتمعات.

---

(*) أبرز مقولات ما بعد الحداثة هو سقوط ما يسميه المفكر الفرنسى جان فرنسوا ليوتاد Metamrratives.. أى الإنساق الفكرية المغلقة، وهى الايديولوجيات التى كانت تنطلق من مسلمات فلسفية محددة كالماركسية Martism.

(**) أول من ابتكر مصطلح (العولمة) هو العالم الكندرى [مارشال ماك لوهان] أستاذ علم اجتماع الاعلاميات فى جامعة تورنتو، عندما قدم مفهوم (القرية الكونية)، ثم تبنى هذا المصطلح (زبيخو بريجنسكى) الذى أصبح فيما بعد مستشار للرئيس الأمريكى (جيلى كارتر) فى الفترة من ١٩٧٧ - ١٩٨٠.

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٢٦ وما بعدها.

فإنه من الأهمية التعرض بشئ من الشرح لماهية هذا المصطلح، الذى استوعب المجتمع الإنسانى وأثر فى الحياة البشرية فى ظل سماء مفتوحة. وماهية الشئ هى تعريفه وذكر ما يعنيه وما يشتمل عليه من جوانب، وما يترتب عليه من آثار.

**( أ ) تعريف العولمة:**

ليس من شك فى أن مفهوم العولمة قد آثار جدلاً واسعاً متشعباً بين الباحثين، وتشكل من ذلك تيارات مختلفة، ومذاهب متعددة حول مفهوم العولمة.

ولعل السبب فى هذا التفاوت والتباين هو اختلاف المرجعيات التى ينتمى إليها هؤلاء الباحثون، وهذا التشعب والتفاوت المذكور دعا أحد الباحثين إلى الخروج بنتيجة مفادها: «إن تعريف العولمة هو أمر شائك وتوجد صعوبات كبرى فى الاتفاق على مثل هذا التعريف، أو القبول بتعريف واحد محدد لهذه الظاهرة التاريخية التى مازالت فى حالة سيولة.

كما أن المعطيات تشير إلى أنه لا ينبغى الاعتقاد، أو الاقتناع بتعريف واحد لظاهرة تاريخية جديدة وغير مستقرة ومتعددة المسارات ومليئة بكل الاحتمالات كالعولمة. ولا يمكن حصر وتحديد العولمة فى تعريف واحد مهما اتصف هذا التعريف بالشمول والدقة، بل أنه من الطبيعى أن يتفاوت فهم الأفراد للعولمة ومضامينها المختلفة»[1].

**• العولمة لغة:**

- العولمة هى الترجمة الحرفية لكلمة (Globalization) وهذه الكلمة تعنى إعطاء الشئ صفة العالمية، والخروج به من نطاق المحلية أو الإقليمية. وأصل هذه الكلمة بالإنجليزية (Globe) وتعنى كرة، كرة أرضية أو كرة جغرافية أو أى

---

(١) عبد الخالق عبد الله – مقالة (العولمة – جذورها وفروعها وكيفية التعامل معها) – مجلة عالم الفكر – الكويت – عدد أكتوبر وديسمبر ١٩٩٩ – العدد الثانى – ص ٥٠.

جسم بشكل كروى. وهى مشتقة من اللاتينية (Globus)، والأشقاق الإنجليزى لكلمة (Globalization) هو من كلمة (Globe) وتعنى كرة أو كرة أرضية أو جغرافية(١)، كما يعنى لفظ (Globe) العالم The Wrld، وفيها عبارة The global village أى القرية العالمية أو الكونية (بمعنى أن دول العالم عندما تصبح وثيقة الارتباط بعضها ببعض من خلال وسائل الاتصال الحديثة فإنها تصبح معتمدة على بعضها اقتصادياً وسياسياً واجتماعياً وثقافياً، ولفظ (Globlly) يعنى على نحو عالمى ولفظ (Gobalist) بمعنى عولمى أى شخص منتمى للعولمة أو مؤمن بالعولمة، ولفظ (Globalism) بمعنى العملية التى من خلالها يحدث تفاعل بين الأسواق والثقافات على مستوى العالم(٢).

- وكلمة العولمة فى اللغة العربية هى مصدر للفعل عولم المشتق من كلمة عالم(٣)، ويتصل بها فعل عولم على وزن فوعلة(٤).

وأيضاً ربما تكون أقرب إلى كلمة العول – بسكون الواو – مصدر عال، وزيدت الميم والهاء للنسب، فيقال عولمة، ومما يساعد على إيراد هذا المعنى أن كلمة العول إما مأخوذة من عال الرجل اليتيم – كلفه – وكأن الدول الغربية فى ظل العولمة هى كفيل الدول النامية، لذلك بسطت نفوذها الاقتصادى والثقافى عليها. أو أنها مأخوذة من الجور والظلم، يقال عال الرجل عولا أى جار وظلم، والعولمة فى مفهومها الاقتصادى هى الهيمنة على السوق العالمى، وإخضاع دول لأخرى(٥).

---

(١) د/ إبراهيم عبد الهادى المليجى، د/ محمد محمود المهدى – العولمة وأثرها فى التخطيط الإجتماعى – المكتب الجامعى الحديث – الإسكندرية – سنة ٢٠٠٥ – ص ١٣.

(٢) د/ هلالى عبد اللاه أحمد – مرجع سابق. هامش ص ٢٦.

(٣) د/ محمد حسن الجبل – لغة القرآن الكريم فى عصر العولمة – الدار المصرية – الإسكندرية – سنة ٢٠٠٠ – ص ٢١٩.

(٤) د/ موسى الضرير – العولمة.. مفهومها.. بعض ملامحها – مقال ضمن مجلة معلومات دولية – العدد (٥٨) مركز المعلومات القومى – سوريا – سنة ١٩٩٨ – ص ٦.

(٥) د/ عبد الهادى محمد زارع – توظيف الاعلام لنقل الخطاب الشرعى الصحيح فى ظل العولمة – (بحث ضمن أعمال مؤتمر العولمة وموقف الفكر الإسلامى منها – كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية) الفترة من ٢٩:٣٠/١١/١٩٩٩ – ص ٩٤.

- وقد كانت أول صياغة لكلمة العولمة فى اللغة الانجليزية فى معجم (Webster's) حيث يعرف الكلمة بأنها:

To globalize; To make, global Esp to make world in scope or application.

وهذا يعنى اكساب الشئ طابع العالمية، وبخاصة جعل نطاق الشئ أو تطبيقه عالمياً[1]، ومن ثم فإن الدعوة إلى العولمة بهذا المعنى إذا صدرت من بلد أو جماعة، فإنها تعنى تعميم نمط من الأنماط التى تخص ذلك البلد أو تلك الجماعة وجعله يشمل الجميع (أى العالم كله)، الخروج من الحيز الاقليمى إلى نطاق العالمية..

- وتعطى المعاجم الفرنسية للكلمة هذا المعنى نفسه تقريباً، فالعولمة (Mondialistion) هى أن يصبح الشئ عالمياً (Modialiser)، أى نقله من المحدود المراقب إلى اللامحدود الذى ينأى عن كل مراقبه. والمحدود هنا هو أساساً الدولة القومية التى تتميز بحدود جغرافية، ومراقبة صارمة للوارد من الخارج (منتج - سلعة - فكر - ثقافة)، أما اللامحدود فالمقصود به (العالم) أى الكرة الأرضية(*).

- ولقد تعرض بعض العلماء للعولمة فذهب رونيه فاليت R. Valette إلى أن العولمة عبارة عن مسلسل تكثيف لتيارات الأفراد والسلع والخدمات والتقنية وانتشارها - بموازاة مع ذلك - تشمل الكرة الأرضية بكاملها. كما يعترف بأن المبادلات الدولية قديمة جداً، إلا أن تكاثفها وكثافتها وتنوعها وشيوعها

---

(1) د/ إبراهيم عبد الهادى المليجى وآخر - المرجع السابق - ص ١٤.

(*) فالعولمة اذن تتضمن معنى الغاء حدود الدولة القومية فى مجال (الاقتصادى - السياسى) وترك الأمور تتحرك فى هذا المجال عبر العالم وداخل فضاء يشمل الكرة الأرضية جميعها. د/ محمد عابد - قضايا فى الفكر المعاصر - مركز دراسات الوحدة العربية، بيروت - ط١ - سنة ١٩٩٧ - ص ١٣٦.

الواسع، قد أدت إلى ظهور كلمة جديدة لتمييز هذا المسلسل هى كلمة العولمة[١].

أما ريكاردو بتريلا R. Petrella فيحدد العولمة بأنها مجموعة المسلسلات التى تمكن من انتاج وتوزيع واستهلاك سلع وخدمات، من أجل أسواق عالمية منظمة (أو ستنظم) بمعايير ومقايس عالمية[٢].

وعلى الرغم من أن العولمة – بحسب دلالتها الاشتقاقية فى اللغات الأجنبية بالذات – لها جذور اقتصادية وعواقب سياسية، إلا أنها قد تجاوزت دائرة الاقتصاد بوصفها ظاهرة كلية متضافرة الآليات ومتعددة الأبعاد، وشمولية التأثير، فالعولمة الآن نظام عالمى، يشمل مجال الاقتصاد والاتصال، كما يشمل أيضاً السياسة والاجتماع والمعرفة والثقافة[٣].

**● العولمة إصطلاحاً:**

ليس من السهولة بمكان أن يتقبل الجميع مفهوماً واحداً للعولمة دون الكثير من الاعتراضات عليه. إذ ان الظواهر الكبرى – كالعولمة – غالباً ما توصف أكثر مما تعرف، فالعولمة مراوغ، ومتعدد الدلالات ومختلف المعانى، وعمومية استخدام المصطلح تجعل من الصعب ايجاد مفهوم خاص له يتمتع بالقبول الجماهيرى شائع الاستخدام والاستعمال، وبالتالى فإن النظرة الذاتية لهذا المفهوم المراوغ لا يجب أن تقتصر على كينونة المصطلح واعتباها كينونة ذاتية مغلقة، بل يجب أن تتجه إلى طبيعة المصطلح وانفتاحه[٤].

---

(١) يحيى اليحياوى – العولمة.. أية عولمة؟ افريقيا الشرق، المغرب، بيروت – سنة ١٩٩٩ – ص١٩.

(٢) المرجع نفسه – ص ٢٠.

(٣) يراجع فى ذلك:

- Robentson, R.: Globalization, London, sage, 1992. pp. 8 - 114.

(٤) محسن أحمد الخضيرى – العولمة.. مقدمة فى الفكر واقتصاد وادارة عصر اللا دولة – مجموعة النيل العربية – القاهرة – طبعة أولى – سنة ٢٠٠٠ – ص ١٥.

كما أنه يضاف إلى ذلك حداثة المصطلح وعدم رسوخ أركانه، مما يجعل من مفهومه أمراً بالغ الغموض، حتى أنه يمكن القول ان صياغة تعريف دقيق للعولمة تبدو مسألة شاقة نظراً إلى تعدد تعريفاتها، والتى تتأثر أساساً بانحيازات الباحثين الايديولوجية، واتجاهاتهم إذاء العولمة رفضاً أو قبولاً[1].

ونخلص بذلك إلى أن العولمة قد اخلت بسلبياتها وايجابياتها مكانة واضحة لدى العديد من الباحثين والدارسين فى مختلف الميادين، لمعرفة أبعاد هذا المصطلح وما يشمله من ظاهرة، فقد اختلفت الآراء حولها فمن الباحثين من يرى ان العولمة ليست موضوع جديد بل أنها ظاهرة مستمرة منذ فجر التاريخ. وإن اختلفت أهدافها ومسمياتها وأدواتها، بينما يرى فريق آخر من الباحثين أن بداية استخدام مصطلح العولمة يرجع إلى فترة السبعينات من القرن الماضى ١٩٧٠، عند صدور كتابين الأول لماك لوهان بعنوان [حرب وسلام فى القرية الكونية]، والثانى ليو يجنيسكى بعنوان: [أمريكا والعصر الألكترونى][2].

وكما اختلف الباحثون فى معرفة أبعاد كلمة العولمة، اختلفوا فى المعنى الاصطلاحى لكلمة العولمة، فذهب البعض إلى أن «العولمة هى الدخول بسبب تطور الثورة المعلوماتية والتقنية والاقتصادية معاً فى طور من التطور الحضارى، يصبح فيه مصير الإنسان موحداً ونازى للتوحد». أو هى «القوى التى لا يمكن السيطرة عليها للأسواق الدولية والشركات متعددة الجنسية». أو هى «العملية التى من خلالها تصبح شعوب العالم متصلة ببعضها فى كل أوجه حياتها ثقافياً واقتصادياً وسياسياً وبيئياً»[3].

---

(١) السيد ياسين – العرب والعولمة – بحوث ومناقشات الندوة الفكرية – مركز دراسات الوحدة العربية – ط ٢ – بيروت – سنة ١٩٩٨، ص ٢٥.

(٢) دكتور/ حسن محمد حسان – التربية وقضايا المجتمع المعاصر – دار الجامعة الجديدة – الإسكندرية – سنة ٢٠٠٦ – ص ٦.

(٣) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية – مرجع سابق – ص ٢٦.

ونظراً لعدم اتفاق الباحثين على تعريف موحد للعولمة، فقد اتجه الكثير من دارسيها إلى تحديد سماتها الرئيسية، والتى تم حصرها فى ثلاثة[1]:

اولها: أن نطاقها الجغرافى يشمل كل أجزاء المعمورة، وأن محتواها التطبيقى يستوعب كل النشاطات والعمليات والاحداث الاقتصادية والثقافية والسياسية والاتصالية التى تغطى سائر أنحاء الكرة الأرضية.

ثانيها: كثافة التفاعل والتأثير والتأثر بين شتى أرجاء العالم، حيث يوجد عدد ضخم ومتشابك من الأطراف والعلاقات والارتباطات التى تؤثر على بعضها البعض.

ثالثها: الاتجاه التدريجى للبشر فى شتى أنحاء المعمورة نحو المزيد من التشابه فى النشاطات والمؤسسات، بل وفى القيم والذوق العام وأسلوب الحياة اليومية.

فالعولمة تسعى إلى تذويب الفواصل والحدود بحيث يصبح الاقتصاد العالمى سوقاً مفتوحة بلا حدود، والثقافة الإنسانية تفتح على بعضها البعض، وتطور عدداً من قضايا الإنسانية المشتركة بحيث تصبح تدريجياً ثقافة عالمية بلا

---

(١) للمزيد بشأن الجوانب المختلفة للعولمة يراجع بالانجليزية:

- Singer (Peter): "One world: The Ethics of globalization Yale univ" Pr. oc Tober, 2002.
- Held (David), Mc Grew (Anthony): "Globalism/anti, - globalism", Polity Pr., Norember, 2002.
- Berger (Peterl.), Hunting, Ton (samuel p.): "Many globalizations: diversity in the contem porary world", Oxford university Press, June, 2002.

وراجع باللغة الفرنسية:

- Thwaites (James D.): "Mondialisation: Origines, develo ppement et Effets", Pr. De L'université Laval, 2000.
- Elbaz (Mikhael): "Mondialisation. Citoyennete et multicura Lisme", Pr. De L'univesite Laval, 2000.
- Sertati (Claude): "Mondialisation armée: Le dese quilibre de La terreur", tex tuel, 2001.

حدود، حتى الشئون السياسية التى مثلت دوماً حدوداً وحصوناً منيعة، يتنبأ البعض أن سطوتها سوف تتراجع مع توسع العولمة ليصبح العالم أرضاً بلا حدود. وتعتمد العولمة فى ذلك على نوعين من المؤسسات هما:

الأول: منظمة التجارة العالمية World Trade organization (W.T.O) وهى أحدى الركائز الأساسية فى نظام العولمة والتى تمارس دوراً رئيسياً فى تحقيقها وتحويل الاقتصاديات المحلية المغلقة على ذاتها إلى اقتصاديات مفتوحة مدمجة فعلياً فى الاقتصاد العالمى(١).

الثاني: شبكة الإنترنت والتى تعد المنبر الرئيسى للعولمة، حيث وفرت سرعة الوصول إلى المعلومة وسرعة انتشارها، وخلقت أنماطاً من التفاعل العلمى لم تكن ممكنة من قبل.

وإذا كانت العولمة تسعى إلى التحرر من كافة القيود التى تحد من قدرات البشر، والتحرر من الصراعات التى فرضتها السياسية، والتحرر من سيطرة الدولة على الاقتصاد والمعلومات، بل والتحرر من التعصب والتحيز ضد أى من بنى البشر على أساس الانتماء لبلد أو دين أو ثقافة أو طبقة اجتماعية كما تسعى العولمة إلى تجانس قوانين الملكية الفكرية Harmonization of intellectual property laws بين الدول من خلال المزيد من القيود عليها. بيد أنه رغم هذه الايجابيات فإن الحركة المضادة للعولمة The Anti - globalization move-ment، ترى على العكس من ذلك أنها ضارة سواء بالنسبة للبيئة أو حقوق العمال أو القيم الإنسانية والروحية، وسواء بالنسبة للأنتماء والهوية والسيادة الوطنية والقومية(٢).

---

(١) فى عام ١٩٩٥ حلت منظمة التجارة العالمية محل اتفاقية الجات التى أنشأت عام ١٩٨٤ من أجل أزالة الحواجز غير الجمركية أمام تبادل السلع والخدمات فيما بين الدول، وكلمة الجات هى الأحرف الانجليزية الأولى للاتفاقية العامة للتجارة والتعريفة الجمركية، وتعد منظمة التجارة العالمية هى المسئولة الأولى عن الادارة والاشراف على تنفيذ اتفاقيات تحرير التجارة بين الدول.

(٢) د/ هلالى عبد اللاه أحمد – مرجع سابق – هامش ص ٢٧.

**(ب) سمات العولمة:**

يرى جانب من الباحثين ان العصر القادم وهو عصر العولمة، سيتسم بسمات عدة، ابرزها ثلاث سمات تتعلق[1] بخصائص ذاتية إنسانية هى:

١- **العلم الغزير** حيث تعدد مصادر المعرفة أكثر مما هى عليه الأن فلن تكون المدرسة أو وسائل الأعلام أو الكتب وحدها مصدراً للمعرفة، بل ستصبح إلى جانبها مصادر أخرى أكثر اتساعاً وشمولاً، فبإستطاعة الإنسان أن يحمل مكتبة كاملة فى جيبه من خلال الاقراص المبرمجة (CD) كما ان المعرفة لن تقتصر على التخصص، وسيصبح تعدد اللغات أداة العصر للمعرفة، وسيكون إلى جانب اللغة (الأم) لغات أخرى.

٢- السمة الأخرى فهى **توفير المهنية العالية**، فالمهارات المهنية يجب أن تكون ذات مستوى متقدم فى الأداة، لأنها ستتعامل مع أجهزة وتقنية عالية تتطلب تعليماً وتأهيلاً وتدريباً عالياً، حيث سيقضى الإنسان ربع وقته تقريباً يتعلم كيف يتعامل مع ذلك التقدم العلمي والاستفادة منه.

٣- أما السمة الثالثة **من سمات عصر العولمة فهي المرونة والتنوع**، وهى سمة ليست مقتصرة على مرونة المادة بل تمتد إلى مرونة الموقف والفكر وتنوعهما، وهذه أخطر القضايا التى تواجه الأمة، حيث يمكن أن تضيع هويتنا الثقافية أو حقوقنا السياسية تحت هذه المظلمة[2].

**(جـ) ثقافة العولمة:**

هى ثقافة احادية القطب تنطوى على معلومات كونية، غايتها إرساء أسس معلوماتية وتقنية لنوع جديد من المجتمعات الإنسانية يدعى بـ (مجتمع

---

(١) د/ إبراهيم عبد الهادى المليجى وآخر - مرجع سابق - ص ١٥.

(٢) سعيد حارب - الثقافة والعولمة دار الكتاب الجامعى - العين - طبعة أولى - سنة ٢٠٠٠- ص١٨، ١٧.

المعلومات) ، يتضمن نمطاً حضارياً احادياً، وفكراً تنموياً احادياً، وتنظماً اجتماعياً احادياً، وطريقا أوحد فى التعامل الدولى، يتضمن المعرفة التقنية والمعلوماتية القائمة على أعمال تشغيل العقل بمعناه الحسابى، والعلم الحديث تقنى فى جوهره أى خاضع لما تقتضيه التقنية بالدرجة الأساسية، أى الكم منهجاً والتحكم والسيطرة غاية.

## الفرع الثالث

### الحق في المعلوماتية.. وتعديلات دستور ١٩٧١ الحالي

جاءت التعديلات الدستورية التى أدخلت على دستور ١٩٧١ الحالى، فى وقت تعاظمت فيه قيمة المعلوماتية، ووصلت تأثيرات ثورة المعلومات والأتصالات إلى مستويات غير مسبوقة، غيرت الكثير فى وجه المجتمعات الحديثة، وأضحى وجودها ومستقبلها رهناً بقدرتها على التحول بل والتطور طوعاً أو كرها صوب مجتمع المعلوماتية، إلا أن هذه التعديلات جاءت مخيبة لآمال المهتمين بالمعلوماتية.

وفى خضم تطور الحياة السياسية للمجتمع فى مصر، وتزامن ذلك مع التعديلات الدستورية التى تم الاستفتاء عليها شعبياً فى ٢٦ مارس ٢٠٠٧، ذهب رأى(١) إلى أن اللافت للنظر أنه لا الدستور الحالى ولا التعديلات التى أدخلت عليه يتعاملان بالأهمية الواجبة مع موضوع (الحق فى الحصول على المعلومات والحق فى حرية تداولها)، الذى يعتبر قضية هامة والعصب الأساسى لأى مجتمع يعيش فى ظل منجزات وتحديات ثورة المعلومات، ويتطلع لتوظيفها فى عملية تنمية بشرية اقتصادية اجتماعية شاملة. ويضيف هذا الرأى أن ما يثير الدهشة والاستغراب أن غياب هذه القضية عن أجندة التعديلات الدستورية

---

(١) الأستاذ/ جمال محمد غيطاس – التعديلات الدستورية... وحق الحصول على المعلومات – (مقالة) بجريدة الأهرام – العدد ٤٣٩٠٥ – ٢٠ فبراير ٢٠٠٧ – ص ١٣.

والفعليات الدائرة حولها لم يحرك ساكناً لدى القائمين على أمور المعلوماتية وتكنولوجياتها والمهتمين بها.

والمأمول – فى مقابل صمت القائمين على قضايا المعلوماتية – أنه كان يجب أن تتضمن التعديلات الدستورية تغييراً نوعياً فى الوضع الدستورى لقضية «الحق فى الحصول على المعلومات والحق فى تداولها» لتصبح ضمن الحقوق المنصوص عليها بكل صراحة ووضوح ودقة فى نصوص الدستور ٧١ المعدل، ثم توضع لها قوانين واجراءات وآليات تضمن تفعيلها عملياً ومجتمعياً.

ويدلل ذات الرأى إلى أن ما يدفعه إلى المطالبة بإدراج حق الحصول على المعلومات وحق تداولها لتصبح ضمن حقوق الإنسان المنصوص عليها دستورياً. أمرين هما:

**الأمر الأول**: أن مواد الدستور ١٩٧١ الحالى البالغة ٢١١ مادة جميعها تتناول قضايا لا تمت لقضية المعلومات بأى صلة، فيما عدا خمس مواد فقط يمكن القول أن لها علاقة بقضية المعلومات بشكل أو بأخر . وهى:

المادة (٤٥) : «لحياة المواطنين الخاصة حرمة يحميها القانون....».

المادة (٤٧) : «حرية الرأى مكفولة، ولكل انسان التعبير عن رأيه ونشره بالقول أو، الكتابة أو التصوير أو غير ذلك من وسائل التعبير فى حدود القانون....».

المادة (٤٨) : «حرية الصحافة والطباعة والنشر ووسائل الإعلام مكفولة....».

المادة (٦٣) : «لكل فرد حق مخاطبة السلطات العامة كتابة وبتوقيعه....».

المادة (٢١٠) : «للصحفين حق الحصول على الأنباء والمعلومات طبقاً للأوضاع التى يحددها القانون. ولا سلطان عليهم فى عملهم لغير القانون».

وبدراسة هذه المواد بدقة وعمق نجدها تعالج قضايا الحق فى المعلومات والحق فى حرية تداولها معالجة هامشية منقوصة، فهى إما تتناولها عن بعد أو

بطريقة غير مباشرة أو بشكل عرضى، أضافة إلى أن معظمها يتعلق بنشر المعلومات وحماية الخصوصية وحرية التعبير أكثر من الحق فى الحصول عليها من مصادرها وحرية تداولها. بل يمكن القول أنه فيما عدا المادة (٢١٠) المتعلقة بحق الصحفيين فى الحصول على الأنباء والمعلومات لا توجد بين مواد الدستور إشارة واضحة ومباشرة لهذه القضية. وخاصة أن – كما هو معلوم – الحق فى الحصول على المعلومات وحرية تداولها لم يعد حقاً مقصوراً على الصحفيين وحدهم، بل لقد امتد هذا الحق لفئات ومؤسسات وهيئات كثيرة بالمجتمع، سواء أكانت مؤسسات مجتمع مدنى أو مجتمع أعمال ومستثمرين أو باحثين وأكاديميين أو منظمات ومؤسسات سياسية... وغير ذلك.

**الأمر الثاني:** أن التعديلات الدستورية المضافة إلى الدستور لم تتعامل مع هذه القضية من الأساس – لم تضم التعديلات وقت طرحها ومناقشتها وأقرارها من السلطة التشريعية، أى نص يشير مباشرة لقضية الحق فى الحصول على المعلومات.. والحق فى حرية تداولها – وتركتها على وضعها الدستورى الذى كانت عليه – قبل التعديلات – المنقوص، الذى لا يناسب مقتضيات التنمية الشاملة فى عصر المعلومات.

وتفسير ذلك: أنه طبقاً للطلب الذى تقدم به رئيس الجمهورية لمجلس الشعب ومجلس الشورى بشأن تعديل ٣٤ مادة من الدستور، فإن المواد المطروحة للتعديل(*) لا يوجد من بينها أى مادة من المواد الخمسة السابق عرضها، بالإضافة إلى أن التعديلات الدستورية – ذاتها – لم تتضمن إضافة أى مواد

---

(*) المواد التى طرحت للتعديل الدستورى هى: ١، ٤، ٥، بإضافة فقرة ثالثة، ١٢ للفقرة الأولى، ٢٤، ٣٠، ٣٣، ٣٧، ٥٦، ٧٨ إضافة فقرة ثانية، ٨٢، ٨٤ الفقرة الأولى، ٨٥ الفقرة الثانية، ٨٨، ٩٤، ١١٥، ١١٨ الفقرة الأولى، ١٣٣، ١٣٧، ١٣٦ الفقرة الأولى، ١٣٨ إضافة فقرة ثانية، ١٤١، ١٦١ إضافة فقرة ثانية، ١٧٣، ١٧٩ الفصل السادس، ١٨٠ الفقرة الأولى، ١٩٤، ١٩٥، ٢٠٥. (للمزيد يراجع دستور ١٩٧١ الحالى مضاف إليه التعديلات الدستورية ٢٦ مارس ٢٠٠٧، المطابع الأميرية – القاهرة – سنة ٢٠٠٧).

تتعلق بهذه القضية، كما هو الحال مع قضية الحفاظ على البيئة. والنتيجة التى تمخض عنها الوضع هى قصر التعديلات الدستورية التى اضيفت لدستور ١٩٧١ الحالى، على ما طلبه رئيس الدولة فقط، ولم تزيد الجهات المعنية بالدراسة والتمحيص - وموائمة الأوضاع فى المجتمع مع متطلبات العصر - عن هذه التعديلات أى نصوص جديدة، وبذلك ظلت الوضعية الدستورية لحق الحصول على المعلومات وحرية تداولها، كما هى بالدستور من ذى قبل دون أى تغيير أو اضافة.

- **النتائج التي يمكن أن تترتب علي عدم أضافة حق الحصول علي المعلومات إلي التعديلات الدستورية(١):**

لا يمكن الحديث عن النتائج المتوقعة بعيداً عن الأهداف المبتغاه من وراء التعديلات الدستورية، فطبقاً لما تم أعلانه، فإن أحد أهم الأهداف التى تسعى إليها التعديلات هو (تحقيق التلاءم بين نصوص الدستور والأوضاع الاقتصادية والسياسية المعاصرة). وقياساً على هذا الهدف فإن النتائج التى ستترتب على التعديلات الدستورية بصورتها التى تمت، سوف تمضى فى مسارين:

**المسار الأول:** هو المسار العالمي. حيث سيكون الدستور بعد تعديله غير متلائم مع الأوضاع العالمية الحاصلة فى هذا الشأن. وأهمها روح وبنود الأعلان العالمى الصادر عن القمة العالمية لمجتمع المعلومات، والتى حضر الرئيس/ مبارك بنفسه دورتها الأولى بجنيف عام ٢٠٠٣، ثم شاركت مصر بوفد وزارى فى دورتها الثانية بتونس عام ٢٠٠٥، ووقعت على الوثائق الصادرة فى هذه القمة وشاركت فى صياغتها. وهى وثائق ركزت بشدة على الحق فى الحصول على المعلومات وحرية تداولها(*).

---

(١) المرجع نفسه.

(*) البند الأول فى إعلان جنيف، تحدث عن الرؤية المشتركة عالمياً لمجتمع المعلومات حيث نص على أن: «مجتمع المعلومات يرتكز على الناس ويستطيع كل فرد فيه أن يخلق المعلومات -/-

ومن ناحية أخرى لن يأتى الدستور متلائماً مع الأوضاع المعاصرة على ساحة حقوق الإنسان، التى تطورت حالياً لتشمل (حقوق الإنسان فى العصر الرقمى ومجتمع المعلومات). وأولها الحق فى الحصول على المعلومات وحرية تداولها باعتباره جزءاً لا يتجزأ من حقوق الإنسان الأساسية التى لا ينبغى التهاون فيها أو غض الطرف عنها.

**أما المسار الثاني:** فهو المسار الوطنى. وفى هذا الصدد نجد أن الأوضاع الاقتصادية المعاصرة تعنى عملياً التغييرات الاقتصادية العميقة التى يمر بها الاقتصاد العالمى حالياً، وتحوله إلى اقتصاد قائم على المعلومات يتطلب تغييراً فى البيئة القانونية والتشريعية التى تحكم تداول المعلومات، بما يعمل على انسيابها بسهولة ودقة بين مراكز وأطراف ووحدات الجهاز الإدارى والاقتصادى والخدمى للدولة، سواء حكومة أو قطاعاً خاصاً، ويوفر للمواطن والمستثمر وصاحب القرار دعماً قوياً من خلال المعلومة الصحيحة فى الوقت المناسب، ويضفى على الاقتصاد قدراً من الشفافية والوضوح، وينفض عنه غبار سنين طويلة من نقص المعلومات وعدم دقتها.

- **المأمول في نطاق الحراك السياسي والتغييرات التشريعية:**

أن يوضع عين الاعتبار وقيد الدراسة والتشريع الحق فى الحصول على المعلومات وحرية تداولها، ضمن قضايا التعديلات الدستورية القادمة(*)، بحيث

---

والمعارف، وأن ينفذ إليها وأن يستخدمها ويتقاسمها». والمعنى هنا أن ركيزة مجتمع المعلومات أن يكون الفرد حراً فى أن يولد ويستخدم ويتقاسم المعلومات.

ثم أكد البند الثانى من الإعلان المعنى نفسه مرة أخرى، حيث نص على أن: «يقوم مجتمع المعلومات الذى نفسره على المبادئ المنصوص عليها فى ميثاق الأمم المتحدة، والإعلان العالمى لحقوق الإنسان، وأن يكون قادراً على تحقيق النفاذ الشامل إلى المعلومات واستخدامها فى خلق المعارف وتجميعها ونشرها».

(*) شملت التعديلات الدستورية التى تم الاستفتاء عليها فى ٢٦ مارس ٢٠٠٧ عدد ٣٤ مادة، تتضمن تعزيز دور البرلمان فى الرقابة على أعمال الحكومة، وإتاحة وقت أوسع لمناقشة الموازنة العامة للدولة والحساب الختامى لها، وتخفيف اجراءات سحب الثقة من الحكومة، وعدم

-/-

يوضع لها نص مستقل فى مادة بذاتها فى الدستور، باعتبار أن هذا الحق يشمل قضية تعد بحق من القضايا الجديدة ذات الأثر الفعال الحيوى على مستقبل المجتمع – وهو يقف على اعتاب الألفية الثالثة (ألفية المعلوماتية) – أسوة بما تم مع قضية الحفاظ على البيئة التى تم صياغة مادة مستقلة بشأنها(*) .

وأحسب أن فكر المساواة دستورياً بين حق الحصول على المعلومات وحرية تداولها، وبين الحفاظ على البيئة، لا ينطوى على أى مبالغة – أو جعل القضية فى حجم أكبر مما تستحق – لأنه إذا كانت قضايا البيئة من القضايا الجديدة على المجتمع، ولم يتناولها الدستور من قبل وتصاغ لها النصوص القانونية للوقوف على حقيقة أمرها وضبط مرتكبيها حماية للمجتمع وتأصيلاً لأمن المواطن وصيانة لحقوقة البيئية. فإن الحق فى المعلومات وحرية تداولها ليست بالقضية الجديدة – المستحدثة – بل هى قضية متعددة الأوجه، عريقة فى جذورها ودائمة ومتطورة وأكثر حيوية لكافة مجالات التنمية، ولا تثريب فى قولنا أن حق المعلوماتية وحرية تداولها، ذو أثر فعال فى الحفاظ على البيئة وممتد لحق الإنسان فى بيئة نظيفة.

---

حل مجلس الشعب أو التقدم بطلب تعديل الدستور، أو إقالة الحكومة فى حالة تولى رئيس مجلس الوزراء المسئولية بديلاً عن رئيس الجمهورية فى حالة وجود مانع مؤقت أو دائم أو الإدانة، ويدخل ضمن التعديلات التيسير على الأحزاب للترشيح لمنصب رئيس الجمهورية بإعداد شروط دائمة للترشيح وشروط مؤقتة خلال المرحلة الانتقالية، وتطبيق إجراءات جديدة لضمان نزاهة الانتخابات، والاشراف القضائى عليها، واختيار نظام انتخابى يضمن تمثيلاً أوفى للأحزاب، ويسمح لمرأة بمشاركة فعالة فى الحياة السياسية، وتعديل بعض أحكام مجلس الشورى، والحفاظ على البيئة.

(*) تضمنت التعديلات الدستورية – التى تم الاستفتاء عليها فى ٢٦ مارس ٢٠٠٧ – المادة (٥٩) وتنص على أن: «حماية البيئة واجب وطنى، وينظم القانون التدابير اللازمة للحفاظ على البيئة الصالحة».

# المطلب الثاني

# عناصــــر المعلوماتيـــة

## الفرع الأول

## الحاســـــب الآلي

نعنى بنظم الحاسبات Computer Systems كل مكونات الحاسب المادية Hard Ware والمعنوية Soft Ware. وشبكات الاتصال الخاصة به Net Works، بالأضافة إلى الأشخاص، والتى يمكن بواسطتها تحقيق وظيفة أو هدف محدد(١).

**تطور جهاز الحاسب الآلي (أجيال الحاسوب):**

تطور جهاز الحاسب الآلى فى عدة نقلات نوعية تمثل أجيال الكمبيوتر، والتى كان الأساس فيها هو التغيير الذى طرأ على العنصر المادى المستخدم فى بناء وحدة المعالجة المركزية والذاكرة، ويمكن أن نعرض لنبذة عن تلك الاجيال على النحو التالى:

- بدأ العمل على أول جهاز رقمى فى العالم عام ١٩٣٧ بمعرفة عالم رياضى من جامعة هارفاد Howard Aiken الذى أنتهى من هذا الإنجاز عام ١٩٤٢ بمساعدة معاونه من تلاميذ ومساعدين وبمشاركة شركة (IBM) التى كانت تقوم فى ذلك الوقت بإنتاج ماكينات جدولة الكروت المثقبة. وكان ذلك الحاسب مثيراً للجدل والإعجاب من ناحية حجمه، فقد كان طوله أكثر من ٥٠ قدم وارتفاعه ثمانية أقدام، واحتوى على حوالى ٧٥٠ ألف جزئى تم توصيلها بما يقرب من ٥٠٠ مفتاح كهروميكانكى(٢).

---

(١) د/ محمد فهمى طلبة وآخرون – الموسوعة الشاملة لمصطلحات الحاسب الاليكترونى – موسوعة دلتا كمبيوتر ٢ – القاهرة – سنة ١٩٩١ – ص ٤٣١.

(٢) فرانك كولسن – ثورة الانفوميديا – ترجمة حسام الدين زكريا – سلسلة عالم المعرفة – الكويت – يناير ٢٠٠٠ – ص ٢٥.

استخدم هذا الجيل الصمام الإليكترونى القادر على تكبير الإشارة الكهربائية، ويعد هذا الصمام كوحدة البناء الرئيسية لتطوير حاسبات ضخمة. تشكل حجماً قياسياً كبيراً، وتزن أطناناً عديدة وتشغل صالات كبيرة مكيفة وتستهلك طاقة كهربية عالية.

- **جيل الكمبيوتر الثاني ١٩٥٨:**

حلت فى هذا الجيل وحدات الترانزستور محل الصمام الإليكترونى، ليصبح الجهاز أصغر حجماً وأسرع وقتاً، وأكفاء فى العمل وأقل استهلاك فى الكهرباء.

- **جيل الكمبيوتر الثالث ١٩٦٤:**

تم أدخال شريحة سيليكون واحدة (Chip) فى هذا الجيل، مقام العديد من وحدات الترانزستور، والعناصر الإليكترونية الدقيقة الأخرى من المقاومات والمكثفات وغيرها، والتى اندمجت بصورة مكثفة داخل البنية البلورية للشريحة المذكورة.

- **جيل الكمبيوتر الرابع ١٩٨٢:**

زاد فى هذا الجيل كثافة العناصر الإليكترونية التى أمكن دمجها فى رقائق السيليكون والتى سميت بالدوائر المتكاملة (Integrated Circuts)، وقد تحقق ذلك بفضل استخدام مواد جديدة ووسائل مبتكرة، فى تصميم وتصنيع هذه العناصر وضبط جودة إنتاجها(١).

ثم تلى هذه المراحل تطور تقنى عالى المستوى فى صناعات الحاسبات والإليكترونيات أمكن بمقتضاه دمج شريحتى المعالج والذاكرة داخل شريحة واحدة بحجم وتكلفة أقل، وبطريقة ترفع قدرات خلايا الذاكرة المؤقتة بالحاسبات أربعة أضعاف، وقدراتها فى الأداء ثمانية أضعاف، وقد وصف هذا التطور بأنه يضع الإنسانية على بداية مرحلة جديدة هى مرحلة المعلوماتية.

---

(١) د/ السيد عاشور – ثورة الإدارة العلمية والمعلوماتية – الجمعية المصرية للحاسب الآلى – القاهرة – سنة ٢٠٠٠ – ص ٢٦.

ومع التطور المعلوماتي برزت نوعية جديدة من شركات الكمبيوتر، لم تقم بتصنيع الأجهزة على الإطلاق لكنها قامت بتصميم أنظمة البرمجيات مثل معالج الكلمات Word Processing والتصميمات التخطيطية (الجرافيك Graphics).

**البند الأول: تعريف الحاسب الآلي:**

تعددت التعريفات التي تناولت الحاسب الآلي(*) .. وهذا ما سوف نعرضه:

أ - **في اللغة:** تعنى كلمة الحاسب بالانجليزية Computer، وقد تعددت الترجمات العربية لهذه الكلمة، فأطلق عليها الحاسوب.. والعقل الاليكتروني.. وأخيراً الحاسب الآلي. وكلمة Computer مشتقة من الفعل Compute أي يحسب أو يحصى، أما الآلة الحاسبة فيطلق عليها Computator(١).

وكلمة Computer في الانجليزية يقابلها في اللغة الفرنسية كلمة Ordinateur أي ناظمة آلية.

ويقصد بالحاسب(**) وفقاً لمعجم الحاسبات عن مجمع اللغة العربية لسنة

(*) بنيت الحاسبات الآلية على فكرة تقليد النماذج بطريقة اليكترونية، تتعامل بالرموز والمعالجة الرياضية، حيث فكر الإنسان لإجراء عملية حسابية مثلاً يلزمه ورقة وقلم (أي طريقة لكتابة وإدخال البيانات)، والتي يقابلها في تصميم الحاسب الآلي وحدة للمدخلات Input unit- يقوم الإنسان باستخدام القلم لتسجيل الأرقام أو بيانات المدخلات على الورقة أي وحدة تخزينية (ذاكرة) تتم عملية معالجة البيانات حسابياً (وحدة حسابية ومنطقية) للحصول على النتيجة مسجلة على الورقة (وحدة للمخرجات Output Unit). للمزيد من التفصيل يراجع:
د/ محمد أحمد فكيرين – أساسات الحاسب الآلي – دار الراتب الجامعي – بيروت – لبنان – سنة ١٩٩٣ – ص ٨، د/ محمد محمد الهادي – تكنولوجيا المعلومات وتطبيقها – دار الشروق – القاهرة – ط١ – سنة ١٩٨٩ – ص ٥٨.

(١) د/ هلالي عبد اللاه أحمد – قانون العقوبات وأزمة الحاسبات – مرجع سابق – ص ٤٧. وقد صدر معجم الحاسبات عن مجمع اللغة العربية سنة ١٩٧٨ بدون إضافة كلمة اليكترونية أو آلية إلى كلمة الحاسبات. والواقع أن عدم إضافة أي نعت أو صفة لكلمة حاسب ربما تكون من قبيل حذف المعلوم، وحذف المعلوم جائز في اللغة العربية.

(**) الحاسب لغة مصدره الفعل حسب أو نحوه، وعلم الحساب.. علم الأعداد وهو من العدد والتدبير والتدقيق.

٢٠٠٣ ، جهاز أو منظومة لتنفيذ مجموعة من العمليات المحددة بتسلسل سبق إعداده، وتشمل هذه العمليات.. عمليات حسابية ومنطقية أو عمليات نقل للبيانات بين أجزاء الحاسب المختلفة وتخزينها واسترجاعها، وقد يعتمد تسلسل العمليات على قيم البيانات المتداولة. ويسمى تسلسل العمليات برنامجاً، وتخزن البيانات والبرامج فى وسط للتخزين يسمى بذاكرة الحاسب(١).

كما يقصد بالحاسب الآلىٰ وفقاً للموسوعية الشاملة لمصطلحات الحاسب الالكترونى: كل جهاز إلكترونى، يستطيع ترجمة أوامر مكتوبة بتسلسل منطقى لتنفيذ عمليات إدخال Data Input أو إخراج Information out put معلومات ، وإجراء عمليات حسابية أو منطقية(*).

ب- أما اصطلاحاً، فقد تعددت تعريفات الحاسب الآلى، وتنوعت مضمنياها ومدلولاتها، فهو عبارة عن مجموعة من الكيانات التى تسمح بدخول المعلومات ومعالجتها وتخزينها واستشارتها أو استرجاعها عند الطلب(٢).

أو هو مجموعة متداخلة من الأجزاء، لديها هدف مشترك، من خلال أداء التعليمات المخزنة(٣).

كما عُرِّف أيضاً بأنه آلة حسابية اليكترونية ذات سرعة عالية ودقة كبيرة، يمكنها قبول البيانات وتخزينها ومعالجتها، للحصول على النتائج المطلوبة(٤). أو هو مجموعة من الأجهزة التى تعمل متكاملة مع بعضها البعض، بهدف تشغيل

---

(١) معجم الحاسبات – ط ٣ – مجمع اللغة العربية – القاهرة – سنة ٢٠٠٣ – ص ٦٦.

(*) يقوم الحاسب بالكتابة على أجهزة الإخراج Output devices أو التخزين. والبيانات يتم إدخالها بواسطة مشغل الحاسب Operator عن طريق وحدات الإدخال أو استرجاعها من وحدة المعالجة المركزية، وبعد معالجة البيانات، تتم كتابتها على أجهزة الإخراج.

(٢) د/ على عبد القادر القهوجى – الحماية الجنائية لبرامج الحاسب – دار الجامعة الجديدة – الإسكندرية – سنة ١٩٩٧ – ص ٣.

(٣) د/ محمد أحمد فكيرين – مرجع سابق – ص ٨.

(٤) المرجع نفسه، ص ٨.

مجموعة البيانات الداخلة طبقاً لبرنامج تم وضعه مسبقاً للحصول على نتائج معينة[1]. كما قيل: إن الحاسب الآلي عبارة عن جهاز اليكتروني يعمل طبقاً لتعليمات محددة سلفاً، ويمكنه استقبال البيانات وتخزينها والقيام بمعالجتها بدون تدخل الإنسان، ثم استخراج النتائج المطلوبة[2].

كذلك يُعرف الحاسب بأنه جهاز اليكتروني يستطيع أن يقوم بأداء العمليات الحسابية والمنطقية للتعلميات المعطاة له بسرعات كبيرة، تصل إلى عشرات الملايين من العمليات الحسابية في الثانية الواحدة، وبدرجة عالية الدقة، وله القدرة على التعامل مع كم هائل من البيانات، وكذلك تخزينها واسترجاعها عند الحاجة إليها[3].

ويطلق البعض على الحاسب تعبير المنظم الآلي، ويعرفه بأنه عبارة عن «جهاز آلي أو آلة تتولى معالجة المعطيات المخزونة في الذاكرة الرئيسية في صيغة معلومات تحت إشراف برنامج مخزون»[4].

أو بصيغة أكثر تفصيلاً، هو آلة يتم تغذيتها بالبيانات (مدخلات) فيقوم بمعالجتها وفقاً لبرامج موضوعة مسبقاً (المعالجة) للحصول على النتائج المطلوبة والتي تخرج (مخرجات) في أي شكل من أشكال المخرجات مثل شاشة العرض أو في صورة تقرير أو في شكل جدول بيانات[5].

---

(١) د/ هدى حامد قشقوش – «جرائم الحاسب الاليكتروني» – مرجع سابق – ص ٦.

(٢) د/ محمد السيد خشبة – «مقدمة في الحاسبات الاليكترونية» – بدون ناشر – القاهرة ١٩٨٤– ص ٢١.

(٣) د/ عزة محمود أحمد خليل – «مشكلات المسئولية المدنية في مواجهة فيروس الحاسب الآلي –. (دراسة مقارنة في القانون المدني والشريعة الإسلامية) رسالة دكتوراه مقدمة لكلية الحقوق – جامعة القاهرة، ١٩٩٤، ص ١٨، د/ حسام محمود لطفي – «الحماية القانونية لبرامج الحاسب الاليكتروني» – دار الثقافة للطباعة والنشر – القاهرة – سنة ١٩٨٧ – ص ٦.

(٤) د/ خالد حمدي عبد الرحمن – «الحماية القانونية للكيانات المنطقية» رسالة دكتوراه مقدمة لكلية الحقوق – جامعة عين شمس، سنة ١٩٩٢، ص ١٦.

(٥) مهندس/ محمد تيمور عبد الحسيب، د/ محمود علم الدين – «الحاسبات الاليكترونية وتكنولوجيا الاتصال» – القاهرة، دار الشروق، الطبعة الأولى، ١٤١٧ هـ – ١٩٩٧م، ص ٤٤.

وأخيراً عرّفت دراسة علمية[1] الحاسب بأنه: «جهاز اليكتروني، يستطيع ترجمة أوامر مكتوبة بتسلسل منطقي، لتنفيذ عمليات إدخال بياناتData input، أو إخراج معلومات Information output وإجراء عمليات حسابية أو منطقية، وهو يقوم بالكتابة على أجهزة الإخراج Output devices أو التخزين. والبيانات يتم إدخالها بواسطة مشغل الحاسب Operator عن طريق وحدات الإدخال، مثل لوحة المفاتيح Keyboard أو استرجاعها من خلال وحدة المعالجة المركزية Central processing unit التي تقوم بإجراء العمليات الحسابية Arithmatic operations، وكذلك العمليات المنطقية Logic operations وبعد معالجة البيانات، تتم كتابتها على أجهزة الإخراج Output devices مثل الطابعات Printers أو وسائط التخزين المختلفة Storage units»[2].

وفي مقام الموازنة بين التعاريف السابقة، يتبين رجحان التعريف الأخير على أساس أنه يستوعب كل الوظائف والمهام التي يؤديها الحاسب الآلي في الحياة العلمية[3].

• **في القانـــون:**

حديثاً – ويمكن القول بأنه حديثاً جداً – وبعد أن أدلى الباحثون بدلوهم في تعريف الحاسب الآلي، وذلك بين أسهاب للبعض واقتصار للبعض الآخر. تدخل

(١) د/ محمد فهمي طلبة وآخرون: مرجع سابق، ص ١٠٨.

(٢) ومما تجدر الإشارة إليه، أن قانون إساءة استخدام الحاسب في المملكة المتحدة Computer misuseact الصادر في ٢٩ يونيو سنة ١٩٩٠ والذي طبق اعتباراً من ٢٩ أغسطس سنة ١٩٩١، لا يحوي تعريفات محددة لمصطلحات «كمبيوتر» «برنامج» أو «بيانات» اعتقاداً من اللجنة التشريعية بأن خطوات التقدم التكنولوجي السريعة سوف تجعل مثل هذه التعريفات عتيقة Outdated راجع:

- Martin WASIK: "Computer crimes and other crimes against information tesnnology in the United Kingdom" R.I.D.P. 1993, p. 631.

(٣) رأى الدكتور/ هلالي عبد اللاه أحمد – المرجع السابق – ص ٥٠.

المشرع المصرى تدخلاً محموداً ليضع تعريفاً للحاسوب بعد قرابه ربع القرن أو أكثر من وجوده على الساحة الدولية، ومن بعدها بقليل الساحة الوطنية.

وقد تضمن القرار بقانون رقم ١٠٩ لسنة ٢٠٠٥ بتاريخ ٢٠٠٥/٥/١٥(*). الصادر بشأن اللائحة التنفيذية للقانون رقم ١٥ لسنة ٢٠٠٥ بشأن تنظيم التوقيع الالكترونى، فى مادة رقم (١):

فى تطبيق أحكام هذه اللائحة يقصد بالمصطلحات الآتية المعانى المبينة- قرين كل منها:

**١٦- الحاسب الآلي:**

جهاز إلكترونى قادر على تخزين ومعالجة وتحليل واسترجاع البيانات والمعلومات بطريقة إلكترونية.

**١٧- برنامج الحاسب الآلي:**

مجموعة أوامر وتعليمات معبر عنها بأية لغة أو رمز أو إشارة، وتتخذ أى شكل من الأشكال، ويمكن استخدامها بطريقة مباشرة أو غير مباشرة فى حاسب آلى لأداء وظيفة أو تحقيق نتيجة، سواء أكانت هذه الأوامر والتعليمات فى شكلها الأصلى أم فى أى شكل آخر تظهر فيه من خلال الحاسب الآلى.

وكما سبق وأوضحنا يتكون الحاسب الآلى من مكونات مادية Hardware ومكونات منطقية Soft Ware، كما أن له شبكات اتصال Networks سلكية ولاسلكية، على المستوى المحلى وعلى المستوى الدولى. وسوف نعرض لذلك خلال الفقرة التالية من الدراسة:

---

(*) الوقائع المصرية – العدد ١١٥ تابع – فى ٢٠٠٥/٥/٢٥.

**البند الثاني: مكونات الحاسب الآلي وشبكات الاتصال الخاصة به.**

**أولاً: مكونات الحاسب الآلي:**

**(أ) المكونات المادية للحاسب الآلي Hardware:**

يمكن تقسيم المكونات المادية Hardware للحاسب الآلى إلى ست وحدات هى: المدخلات – الذاكرة الرئيسية – الحساب والمنطق – التحكم(*) – المخرجات – والتخزين.. وفيما يلى شرح لهذه الوحدات بالقدر الذى يفيد البحث.

**(١) وحدة المدخلات (وحدات الإدخال) Input Units:**

وهى الوسائل التى تستخدم فى إدخال البيانات والبرامج إلى وحدة التشغيل المركزية وذلك بتوجيه من وحدة التحكم. ومن أهم هذه الوسائل(**): –

- **لوحة المفاتيح Keyboard:**

تعتبر لوحة المفاتيح من أهم وحدات الإدخال فى الحاسب، وتستخدم فى إدخال البيانات والأوامر. ومفاتيحها تشبه إلى حد ما مفاتيح الآلة الكاتبة. وتنقسم هذه اللوحة إلى **ثلاثة أقسام:**

---

(*) ويدمج البعض وحدة الذاكرة الرئيسية ووحدة الحساب والمنطق تحت مسمى وحدة التشغيل المركزية Central Processing unit على أساس أن وحدة التشغيل المركزية CPU تمثل عقل الحاسب (د. محمد فهمى طلبة وآخرون: «فيروسات الحاسب وأمن البيانات، موسوعة دلتا كمبيوتر، القاهرة، مطابع المكتب المصرى الحديث، سنة ١٩٩٢، ص ٥٣).
بل إن هناك من يدرج تحت مسمى وحدة التشغيل المركزية بالإضافة إلى وحدتى الذاكرة الرئيسية والحساب والمنطق وحدة التحكم التى تقوم بتنظيم سريان المعلومات وتبادلها بين أجزاء الحاسب المختلفة (م. محمد تيمور عبد الحسيب، د/ محمود علم الدين، المرجع السابق، ص ٤٨ – ص ٤٩).

(**) وذلك بخلاف أجهزة تلقى الرسائل من الأجهزة سواء كانت حاسبات أو أجهزة تلكس أو فاكس.

اولها: قسم مفاتيح الآلة الكاتبة Typerwriter Key Area وموجود به مفاتيح الحروف الأبجدية باللغة الإنجليزية، بالإضافة إلى حروف اللغة العربية فى بعض الأنواع. بالإضافة إلى بعض المفاتيح الخاصة Special Keys.

وثانيها: قسم مفاتيح الوظائف الخاصة Function Keys وهذه النوعية من المفاتيح تؤدى وظائف خاصة تتوقف على طبيعة البرنامج التطبيقى المستخدم.

وثالثها: قسم المفاتيح الرقمية Numeric Keypoard ومفاتيح هذا القسم من الأرقام والعلامات الحسابية مماثلة فى توزيعها لتلك الموجودة على الآلة الحاسبة Calculator بالإضافة إلى بعض المفاتيح الخاصة(١).

- **شاشات اللمس Touch Sereen:**

تسمح هذه النوعية من الشاشات للمستخدم بإدخال بعض البيانات عن طريق لمس مناطق حساسة من الشاشة.

- **نظام الإدخال المرئي Machine Vision System:**

وبالنسبة لهذه النظم، تستخدم كاميرا فيديو Video Camera لالتقاط صور وتحويل تلك الصور إلى أرقام أو إلى إشارات لتقارن بالصور المخزنة لدى الحاسب.

- **نظام الإدخال الصوتي Voice Input System:**

فى هذا النظام يستخدم ميكرفون أو تليفون لتحويل الصوت البشرى إلى إشارات كهربائية ترسل الإشارات إلى الحاسب، الذى يقارن الإشارات التى وصلت إليه بالإشارات المخزنة لديه فى حالة العثور على إشارة ما يتم فهم الكلمة وأداء المطلوب منه.

---

(١) للمزيد بشأن مكونات لوحة المفاتيح يراجع:
د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٥١ – هامش ١، ٢، ٣.

• نظام الفأرة Mouse System:

نظام الفأرة أو المتجول، عبارة عن جهاز متصل بالحاسب الآلى بواسطة توصيلة سلكية Cable أو لا سلكية. ويستخدم هذا النظام والذى يشبه الفأرة، فى تحريك المؤشر على الشاشة، ويتم تحريكه باليد على سطح مستوٍ وتحريكه بهذه الطريقة يؤدى إلى تحريك عجلات مثبتة أسفله، يتم عن طريقها تحريك المؤشر على الشاشة. ويفيد ذلك فى التعامل مع القوائم التى تظهر على الشاشة، حيث يتم تحريك المؤشر إلى الأمر أو الرقم المطلوب ثم الضغط على المفتاح الموجود على الفأرة فيتم تنفيذ المطلوب.

• نظام القلم الضوئي Light Pen System:

نظام القلم الضوئى، عبارة عن جهاز اليكترونى حساس للضوء، يساعد المستخدم على التحكم فى الشاشة، وذلك بتحريك أجزاء من الشاشة أو تغيير حجمها أو ألوانها أو تنفيذ أى عملية مطلوبة حسب البرنامج المستخدم. وذلك عن طريق قوائم تظهر على الشاشة. ويقوم الحاسب بتحديد مكان القلم على الشاشة نتيجة سقوط الضوء عليه، كما أنه يستخدم أيضاً فى الرسم مباشرة على شاشة الحاسب.

• نظام القراءة الضوئية للحروف:

**Optical Character Recopgnition system**

يستخدم هذا النظام من نظم الإدخال فى حالة وجود حجم كبير من الوثائق، ومثال ذلك، تصحيح أوراق الامتحانات لإدخال درجات الطلاب وبيانات الاستفسار عنهم.

• نظام قراءة الحروف المغناطيسية Magnetic Ink Character أو نظام التعرف علي الحروف المكتوبة بحبر مغناطيسي Magnetic Ink Character Recog-nition (MICR):

يستخدم هذا النظام على وجه الخصوص فى البنوك، وذلك لمعالجة الحجم الكبير من الشيكات الصادرة كل يوم. وهو عبارة عن عملية فك شفرة الحروف المغناطيسية المكتوبة على شيكات البنك. ويتم ذلك عن طريق تجميع عدد كبير جداً من الشيكات وإدخالها إلى وحدة القراءة والفرز Reader - sorter unit، حيث تمر الشبكات على مجال مغناطيسى يؤدى إلى شحن الحروف مغناطيسياً. ثم تمر على رؤوس قراءة تقوم بترجمة هذه الحروف. ويمكن إدخال هذه البيانات مباشرة إلى جهاز حاسب لتشغيلها[1].

• **نظام الشرائط أو الأحزمة المغناطيسية Magnetic Stnipes:**

يعتبر هذا النظام أحد الوسائل الهامة لإدخال البيانات إلى جهاز الحاسب بسرعة وبدقة. وذلك باستخدام شرائط مغناطيسية يتم تثبيتها على كروت بها شفرة وبيانات معينة مثل رقم الحاسب أو الكود الشخصى. وهى تستخدم أيضاً فى الأماكن التى يراد إحاطتها بدرجة عالية من السرية، حيث يقوم أى إنسان يحمل كارت تصريح الدخول بإدخال هذا الكارت، الذى يحتوى على كود معين يتم التعرف عليه بواسطة جهاز قراءة الكروت، وفى هذه الحالة يسمح له بالدخول[2].

• **نظام علامات الترقيم أو شفرة الأعمدة Bar Codes:**

يرتكز نظام علامات الترقيم أو شفرة الأعمدة التى توجد على المعلبات على شفرة خاصة تعتمد على خطوط تختلف فى سمكها والمسافات بينها، بحيث يمكن قراءتها بجهاز حساس للضوء. وتستخدم هذه الشفرة فى بعض المحلات التجارية لتعريف السلع وأسعارها، حيث يتم قراءة الشفرة وتحويلها إلى الحروف والأرقام المناظرة[3].

---

(١) د/ محمد فهمى طلبة: «الموسوعة الشاملة لمصطلحات الحاسب الاليكترونى»، مرجع سابق – ص ٢٨٣.

(٢) المرجع السابق – ص ٢٨٤.

(٣) نفس المرجع ـ ص ٢٥٠.

• نظام يد أو ذراع ألعاب الحاسب Joystick:

يستخدم يد أو ذراع ألعاب الحاسب، لتحريك الأشكال والصور على الشاشة. وهو يغنى عن استخدام مفاتيح الاتجاهات على لوحة المفاتيح Keyboard، ويمتاز عنها بإمكانية تحريكه فى جميع الاتجاهات بسرعة كبيرة(١).

• نظام إدخال الأشكال والرسومات:

يتم إدخال الأشكال والرسومات عن طريق لوحة رسومات Graphics table تتكون من مادة شبه موصلة Semi - Conductor تستخدم فى الرسم عليها، ثم تقوم بترجمة الرسوم والأشكال إلى إشارات Digital رقمية تستقبل بواسطة الحاسب.

- الكاميرات الرقمية Digital Cameras:

تعد الكاميرات الرقمية أحدث طرق إدخال الصور إلى ذاكرة الحاسبات الأليكترونية، وهى تعتمد على شرائح ذات حساسية للضوء تسمى Charge Coupted Devices CCD وتحول هذه الشرائح الضوء إلى إشارات رقمية مناظرة. وهى بذلك تختلف عن كاميرات التصوير الفوتوغرافى التى يعتمد عملها على تأثير الضوء الكيميائى على أملاح الفضة (هاليد Halide)(٢).

(٢) وحدة الذاكرة الرئيسية Main Memory (M.M)(٣):

تستخدم الذاكرة الرئيسية لحفظ البيانات والمعلومات والبرامج حفظا دائماً أو مؤقتا. وهى بهذا المعنى تتكون من نوعين:

• النوع الأول: ذاكرة القراءة فقط Read only memory (ROM):

وهى ذاكرة يمكن القراءة منها فقط. وتستخدم لتخزين البيانات والأوامر

---

(١) نفس المرجع، ص ٢٥٠، ص ٢٥١.
(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٥٥.
(٣) المرجع نفسه – ص ٥٦.

بصفة دائمة عند تصنيعها. ولذا تسمى أيضاً بالذاكرة الدائمة Permanenet memory، ومن أهم خصائص هذه الذاكرة، أن برامجها لا تكتب إلا بمعرفة الشركة المنتجة، مثل ذلك لغة المترجم Language interpreter وبرامج بداية التشغيل Start up porgrams ومن خصائصها أيضاً، أنها لا تقبل تخزين أى بيانات بها بعد تصنيعها، ولذا لا يمكن لمستخدم الجهاز أن يسجل فيها أية معلومات، كذلك فإنها لا تفقد ما بها من برامج عند انقطاع أو فصل التيار الكهربائى منها، لأن المعالجة الصناعية تجعلها تحتفظ بمحتوياتها بصفة دائمة.

- **النوع الثاني: ذاكرة القراءة والكتابة Random Access Memory (RAM):**

وهى الذاكرة التى يستعملها المستخدم. وهى تستخدم فى جميع أغراض التخزين أثناء تشغيل الحاسب. فهى المكان الأمثل للتعامل مع البيانات والبرامج. ولذا تسمى أيضاً ذاكرة العمل Working Memory كما تسمى بالذاكرة المؤقتة Temporary memory لأن محتوياتها تتغير حسب البرامج التى يتم تحميلها بالحاسب.

بل ويطلق عليها كذلك الذاكرة العشوائية أو ذاكرة الوصول العشوائى، لأنه من خلالها يمكن الوصول إلى أى عنوان فيها دون حاجة إلى المرور على العناوين الأخرى.

ومن أهم خصائص هذه الذاكرة، أنها تفقد ما بها من برامج وبيانات عند انقطاع مصدر الطاقة، سواء عن قصد بإيقاف تشغيل الحاسب أو بدون قصد، نتيجة لانقطاع التيار ومن خصائصها أيضاً تخزين البيانات Data المدخلة إلى الجانب والتعليمات اللازمة لمعالجة هذه البيانات User programs، وتخزين نتائج عمليات المعالجة تمهيداً لإخراجها، كذلك تخزين البرامج الخاصة بنظام التشغيل Operating System.

(٣) وحدة الحساب والمنطق Arithmetic and logic unit (ALU)[1]:

وحدة الحساب والمنطق هى جزء من وحدة المعالجة المركزية Central processing unit (CPU) وهى المسئولة عن معالجة البيانات حسابياً ومنطقياً. وتتكون وحدة الحساب والمنطق من مجموعة من الدوائر الإليكترونية المنطقية التى يتم توظيفها لأداء العمليات ومجموعة من المسجلات Registers وهى ذاكرة سريعة، تستخدمها هذه الوحدة لاستيعاب البيانات التى يجرى معالجتها.

ومن أهم وظائف وحدة الحساب والمنطق إنجاز العمليات الحسابية Arithmetic operation بواسطة دوائر حسابية مثل الجمع والطرح والضرب والقسمة وتنفيذ تلك العلميات وفق ترتيب محدد مسبقاً وتحت إشراف وحدة التحكم وأيضاً إنجاز العمليات المنطقية Logical operations وذلك عن طريق مقارنة القيمة الرقمية وفقاً لتعليمات.

(٤) وحدة التحكم Control Unit:

تعتبر وحدة التحكم أساس عمل وحدة المعالجة المركزية CPU، فهى التى تقوم بالتنسيق بين وحدات الحاسب الأخرى وضبط كافة التعليمات التى تتم داخل وحدة المعالجة المركزية بإرسال إشارات إلى كل الوحدات المعنية بالأمر.

وتستعين وحدة التحكم فى القيام بوظيفتها، بعدد من المسجلات كذاكرة مؤقتة، ويطلق على أحد هذه المسجلات اسم مسجل العمليات Instruetion Register كما تستعين أيضا بساعة منطقية تقوم بالتحكم فى توقيت العمليات المختلفة.

(٥) وحدة المخرجات ( وحدات الإخراج) Output Units:

وحدة المخرجات أو وحدات الإخراج هى الوسائط المستخدمة لإظهار نتائج التشغيل ومعالجة البيانات. ومن أهم هذه الوسائط ما يلى:

---

(١) المرجع نفسه – ص ٥٧.

• الشاشة Monitor:

وتسمى أيضا وحدة العرض المرئى Video Display Unit (VDU) وهى تعتبر من أهم أجزاء الحاسب استخداماً. إذ عن طريقها يتم استعراض أى بيانات أو معلومات تكتب على لوحة المفاتيح بواسطة المستخدم. كما يتم استعراض البيانات التى تم إدخالها أو المعلومات الناتجة عن معالجة البيانات فى وحدة المعالجة المركزية وكذلك التعليمات الموجهة للمستخدم بواسطة البرامج التطبيقية.

• الطابعة Printer:

والطابعة عبارة عن جهاز يستخدم فى إخراج نسخ مطبوعة من البيانات، مثل التقارير، والشبكات وقوائم البرامج.

• المصغرات الفيلمية Micro filmed printers:

يمكن تخزين المعلومات على أقلام مصغرة، حيث تستخدم تكنولوچيا الميكروفيلمية لمخرجات الحاسب Computer output to micro film لتسجيل المعلومات على فيلم مصغر، حيث من الممكن تصغير الصفحة ٤٨ مرة.

• الراسم Plotter:

هو جهاز يستخدم فى طباعة الرسوم بدرجات وضوح مختلفة على ورق وبالألوان. ومن أشهر أنواع الرواسم.. راسم الطاولة وراسم الاسطوانة.

(٦) وحدات التخزين الثانوية Secondary Storage Units:

قد تكون كمية المعلومات المراد تخزينها كبيرة بدرجة لا يمكن خزنها فى وحدة التخزين الرئيسية، أى الذاكرة الرئيسية، لذا فإن الأمر يتطلب وحدات تخزين ثانوية أو إضافية بقصد التوسع فى طاقة وحدة التخزين الداخلية. وتنقسم وحدات التخزين هذه إلى نوعين: .

**أولهما:** وحدات التخزين المباشر، بمعنى أن أى بيان مسجل على هذه الوسائط يمكن الوصول إليه مباشرة دون الحاجة إلى قراءة البيانات المسجلة عليه من البداية حتى البيان المطلوب. ويتمثل هذا النوع فى الأقراص المغناطيسية.

**ما النوع الثاني فهو:** وحدات التخزين التتابعية، بمعنى أنه من أجل الوصول إلى أى بيان مسجل على هذه الوسائط يجب قراءة الشريط من بدايته إلى المكان الذى يوجد عليه البيان المطلوب. ويتمثل هذا النوع فى الأشرطة المغناطيسية.

وفيما يلى نتحدث عن الأقراص المغناطيسية Magnetic disks والأشرطة المغناطيسية Magnetic Tape باعتبارهما أهم وحدات التخزين الثانوية[1]:

**• الأقراص المغناطيسية Magnetic Disks:**

تعتبر الأقراص المغناطيسية من أفضل أنواع الوسائط التى يمكن استخدامها للتخزين المباشر أو العشوائى، لأنها تتميز بقدرتها الاستيعابية العالية وسرعة تداول المعلومات المخزنة عليها. ومن أهم خواصها إمكانية القراءة أو التسجيل على أى قطاع من السطوح.

وتوجد أنواع عديدة من الأقراص المغناطيسية، لعل من أهمها:

**- القرص المرن Floppy disk:**

يعتبر القرص المرن أشهر وسائط تخزين البيانات. وينتشر استخدامه فى الحاسبات الصغير Micro Computers والمتوسطة Mini Computers وذلك نتيجة سهولة استخدامه وتداوله.

**• القرص الصلب Hard - Disk:**

القرص الصلب عبارة عن قرص معدنى رقيق ومغطى بمادة قابلة للمغنطة. ويلاحظ أن طبقة التغطية لهذا القرص تتم على سطح صلب يتم صنعه

---

(١) لمزيد من الاستفاضة راجع: د/ محمد أحمد فكيرين، مرجع سابق، ص ٨٥ وما بعدها، د/محمد محمد الهادى: مرجع سابق، ص ٩٣ وما بعدها.

من سبائك الألمونيوم، ومن هنا جاء تسميته بالقرص الصلب. ومن خواص هذا النوع السعة التخزينية، وكذلك سرعة تسجيل واسترجاع البيانات التى تفوق سرعة الأقراص المرنة. كما يتميز القرص الصلب أيضاً بعدم إمكانية تحريكه من مكانه ولذا يطلق عليه أحياناً القرص الثابتFixed disk.

- قرص الخرطوش أو قرص الكارتريدج Cartridge - Disk:

وهو قرص هجيني، يجمع بين خصائص القرص الصلب، من حيث كبر حجم السعة التخزينية، وبين القرص المرن فى إمكانية تغيريه من مكانه بقرص آخر.

● الأشرطة المغناطيسية Magnetic Tape:

الشريط المغناطيسى، عبارة عن شريط بلاستيك مغطى بمادة معدنية قابلة للمغنطة Magnetic Oxide ويبلغ عرضه من ربع إلى نصف بوصة. والشريط المغناطيسى قد يكون ملفوفاً على بكرة كبيرة Reel مثل تلك التى تستخدم فى أجهزة التسجيل الصوتى Tape recorder، وقد يكون داخل علبة على هيئة شريط الفيديو أو شريط الكاسيت(١).

(ب) المكونات المنطقية للحاسب الآلي Computer Software(٢):

لعله قد استبان لنا مما سبق، أن وظيفة الحاسب الآلى، هى تنفيذ مجموعة من الأوامر فى ترتيب معين للوصول إلى حل مشكلة ما. ويتم تنفيذ هذه الأوامر على بيانات الإدخال التى تعطى للحاسب.

والبيانات Data هى مجموعة من الحقائق التى تعبر عن مواقف وأفعال معينة، سواء أكان ذلك التعبير بالكلمات أم الأرقام أم الرموز ولا تفيد هذه

---

(١) د/ محمد أحمد فكيرين، المرجع السابق، ص ٨٦، د/ محمد محمد الهادى – المرجع السابق – ص ٩٣ وما بعدها.

(٢) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٦٥.

البيانات فى شئ وهي على صورتها الأولية، لذلك يستدعى الأمر تحليل هذه البيانات وإجراء العمليات الحسابية والمنطقية عليها، أو بمعنى آخر معالجة البيانات Data processing للاستدلال منها على مجموعة من المعلومات Information المفيدة فى اتخاذ القرارات(*).

**(١) تعريف البرامج أو الكيانات المنطقية للحاسب:**

- **التعريف اللغوي:**

يعرف البرنامج أو الكيان المنطقى لغة، بأنه كلمة تستخدم للدلالة على جميع المكونات غير المادية لنظام الحاسب، ويشمل ذلك: برامج النظام أو الكيانات المنطقية الأساسية وهى البرامج الضرورية أو اللازمة لتشغيل الحاسبات وبرامج التطبيقات أو الكيانات المنطقية التطبيقية ويقصد بها البرامج الخاصة

---

(*) هناك تنظيم هرمى خاص للبيانات، حيث يتكون البيان من مجموعة ملفات Files وكل ملف ينقسم إلى مجموعة من السجلات Records والتى تنقسم بدورها إلى مجموعة من الحقول Fields.

والملف هو عبارة عن مجموعة من الوحدات المنظمة على أساس منطقي، كل منها يتألف من مجموعة منه متماثلة من المعطيات، من حيث النوع أو العدد والوصف. فى حين أن السجل هو وحدة الملف، ويتكون السجل من مجموعة من المفردات المتعلقة بموضوع معين، أما الحقل فهو أصغر وحدة يتكون منها الملف، والحقل هو مفردة معينة يتكون منها السجل. والحقل يتكون من مجموعة من الحروف أو الأرقام المترابطة أو الرموز الخاصة لوصف مفردة معينة فى السجل.

وهناك عدة تقسيمات للملفات. إذ يمكن تقسيمها من حيث أسلوب تنظيم البيانات إلى نوعين، أولهما: ملفات تتابعية Sequential files وفيها نجد أن السجلات تتبع بعضها بعضا بطريقة تتابعية تعين عادة باستخدام حقل أو أكثر من حقول المفاتيح ضمن كل سجل. ويستخدم هذا النوع عندما يكون حجم المعاملات كثيراً. أما النوع الثانى فهو: الملفات المباشرة أو العشوائية Direct Files، وملفات هذا النوع لا يمكن استخدامها إلا باستخدام أدوات خزن ووصول مباشرة كالقرص المغناطيسى، بإنشاء علاقة مباشرة بين مفاتيح السجلات المنطقية ومواقعها الطبيعية على القرص.

للمزيد يراجع: د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٦٦.

بمستخدم الحاسب أو البرامج التى تهدف إلى حل المشاكل المتعلقة باستعمال الحاسب الآلى(١).

• التعريف الاصطلاحي:

يعرف بعض الكُتاب البرنامج أو الكيان المنطقى، بأنه عبارة عن: تعليمات مكتوبة بلغة ما موجهة إلى جهاز تقنى معقد، يسمى بالحاسب الإليكترونى بغرض الوصول إلى نتيجة معينة(٢). أو هو مجموعة من التعلميات المتتابعة بصفة منطقية التى توجه إلى الكمبيوتر لأداء عمل أو أعمال معينة(٣)، أو هو مجموعة من الأوامر والتعليمات لأداء العمليات المنطقية المطلوبة(٤).

وعلى نفس المنوال، عرّف القانون الأمريكى الصادر سنة ١٩٨٠ والخاص بحماية حق المؤلف البرنامج Soft Ware بأنه: مجموعة توجيهات أو تعليمات ويمكن للحاسب استخدامها بشكل مباشر أو غير مباشر للوصول إلى نتيجة معينة(٥).

(٢) أنواع البرامج أو الكيانات المنطقية للحاسب:

تنقسم برامج الحاسب الآلى إلى نوعين: أولهما برامج النظام أو الكيانات المنطقية الأساسية، وبرامج التطبيقات أو الكيانات المنطقية التطبيقية، وذلك كما يلى:

---

(١) راجع: «معجم الحاسب» إصدار مجمع اللغة اللغة العربية بجمهورية مصر العربية، سنة ١٩٨٧.

(2) Marilyn (Bohl): Information processing Third ed. Chicago, 1981, p.25.

– دكتور/ حسام لطفى، المرجع السابق، ص ٧ وما بعدها، د. عزة محمود أحمد خليل، المرجع السابق، ص ٣١.

(٣) د/ محمد الهادى، المرجع السابق، ص ١١٠.

(٤) د/ خالد أبو الفتوح فضالة – «مدخلك إلى فيروسات الحاسب – المرجع السابق، ص ٢٦، انتصار نورى الغريب، المرجع السابق، ص ٨٥.

(5) "Copyright protection of computer program object cobe", Harvard low review, vol. 96, June 1983, p. 1723.

– د/ عزة محمود أحمد خليل، المرجع السابق، ص ٣٢.

**النوع الأول: برامج النظام أو الكيانات المنطقية الأساسية:**

تعمل برامج النظام System Programs فى الأساس لتساعد الحاسب على التشغيل. ذلك أن الأعمال الداخلية للحاسب معقدة للدرجة التى لا نستطيع معها التعامل مع الحاسب مباشرة بدون استخدام برامج تساعدنا على التعامل معه، وهذا ما تقوم به برامج النظام. وهى تشمل[1]: نظم التشغيل Operating Systems والبرامج المساعدة Utility programs ونظم إدارة قواعد البيانات Data Base management بالإضافة إلى برامج ترجمة اللغات Compilers.

والواقع أن برامج النظام تقوم بالعديد من المهام، لعل من أهمها الإشراف ودعم التشغيل الرئيسى للجهاز الذى يشمل الخدمات الجوهرية، التى تحتاج إليها وتستعملها برامج التطبيقات مثل الجداول الاليكترونية Spread sheets ومعالجة الكلمات Ward Processing، كذلك التحكم والسيطرة على مكونات الحاسب، وأداء العمليات الأساسية التى تساعد المستخدم على التعامل مع هذه المكونات لنسخ الملفات ومسحها ونسخ الأقراص وتشكيلها، وذلك باستخدام مجموعة من الأوامر Commends يسهل على المستخدم حفظها والتعامل مع الحاسب من خلالها.

ومن مهام برامج النظام أيضاً، السماح لعدة مستخدمين بالتعامل مع نفس الحاسب فى ذات الوقت. بالإضافة إلى التعامل مع شبكات الحاسب التى تستخدم وحدات طرفية بعيدة Remote Terminals.

**النوع الثاني: برامج التطبيقات أو الكيانات المنطقية التطبيقية:**

برامج التطبيقات Application Program Soft Ware هى البرامج التى تصمم للقيام بمهام محددة. ومن أمثلة ذلك.. برامج معالجة الكلمات والنصوص

---

(١) د/ محمد فهمى طلبة وآخرون - «الموسوعة الشاملة لمصطلحات الحاسب الاليكترونى - مرجع سابق، ص ٤٣٥.

Ward Processing التى تستخدم الحاسب كآلة كاتبة متطورة، وبرامج قواعد البيانات Data Base(*)، والجداول الاليكترونية Sperad Sheet(**).

**وهناك طائفتان من برامج التطبيقات:**

الأولى: برامج التطبيقات سابقة التجهيز Ready-made application pack-ages. هى تلك البرامج التى خططت وكتبت للتحكم فى معالجة وحل مهمة خاصة. وتنقسم إلى البرامج التطبيقية ذات الوظيفة الواحدة، وتشمل برامج أدارة المواد البشرية، والبرامج التطبيقية ذات الوظائف المتكاملة، وهو عبارة عن وحدة واحدة تحتوى على مجموعة من البرامج المركبة التى تؤدى وظائف يكمل بعضها بعضاً.

الثانية: برامج التطبيقات طبقاً لاحتياجات العميل – User - developped application programs هى تلك البرامج المعدة طبقاً لاحتياجات العميل، أو هى البرامج التى يعدها خبير البرمجة Programmer خصصياً لعميل معين بناء على اتفاق مع هذا العميل لتكون صالحة للوفاء بحاجة منشأته، فهى برامج تفصل حسب رغبة وحاجة العميل.

**ثانياً: شبكات اتصال الحاسب الآلي:**

يقصد بالشبكة Network اتصال جهازين أو أكثر من أجهزة الحاسب الآلى اتصالات سلكياً أو لاسلكياً. أو هى حزمة من أجهزة الحاسبات المتصلة معاً، وقد تكون الأجهزة موجودة فى نفس الموقع فتسمى شبكة محلية Local Area net-

(*) تسمى بالفرنسية Basa de données. وهى عبارة عن ملفات المعطيات المخزونة فى الحاسب، ولكنها مرتبة بحيث يمكن نيلها بطرق عديدة مختلفة للاستعمال فى تطبيقات متنوعة. والفكرة هى أن تخزن المعطيات نفسها مرة واحدة ولكن يمكن مداولتها بواسطة نظام ادارة قاعدة البيانات، بحيث يمكن لأجزاء مختلفة من البرمجيات أن تشارك فى ملفات المعطيات.

(**) تسمى بالفرنسية Programme de Calcul de tableau. والجدول الاليكترونى عبارة عن جدول مكون من عدد كبير من الأعمدة والصفوف التى يتم من خلالها إدخال البيانات وإجراء عمليات تخزين هذه البيانات واسترجاعها أو طباعتها فى أى وقت، كما يتيح للمستخدم اجراء عمليات حسابية معقدة والحصول على أدق النتائج.

work (L.A.N)، كما قد تكون موزعة في أماكن متفرقة، ويتم ربطها عن طريق خطوط التليفون وتسمى في هذه الحالة شبكة واسعة النطاق، أو شبكة ممتدة(*)(١).

**البند الثالث: النظم المطمورة Embedded Systems:**

**أولاً: تعريف النظم المطمورة:**

النظم المطمورة تعني الشرائح الاليكترونية المبرمجة Micro - Chips، وقد يطلق عليها البعض أنظمة داخلية مضمنة أو النظم المضمنة أو النظم المدمجة(٢).

**ولغة:** المطمورة حفيرة تحت الأرض، أو مكان تحت الأرض قد هيئ خفياً يطمر فيها الطعام والمال (المعنى: يخبأ)، وقد طمرتها أى ملأتها، والمطامير حفر تحفر في الأرض توسع أسافلها تخبأ فيها الحبوب(٣).

وفي حديث الحساب يوم القيامة، يقول العبد: عندى العظائم المُطمرات، أى المُخبآت من الذنوب(٤).

**وورد في معاجم اللغة العربية في مادة ط م ر(٥):**

طمر البئر طمراً (دفنها)، وطمر نفسه وطمر الشئ أو المتاع: (خبأه وأخفاه)، وطمر في الأرض طموراً (ذهب)، وطمر إذا تغيب واستخفى.

---

(*) Wide Area Net Work .. ولكي يتم إرسال بيانات الحاسب عن طريق خطوط التليفون، لابد من تحويل إشارات رقمية إلى إشارات تناظرية، ثم إعادة تحويلها عند الطرف الآخر.

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٧٦.

(٢) سامى شلبى - مواجهة أزمة الكمبيوتر عام ٢٠٠٠ فى الواقع العربى (إخماد عاصفة القرن) - القاهرة - الشركة العربية للاعلام العربى (شعاع) - ط١ - سنة ١٩٩٨ - ص ٢١ وما بعدها.

(٣) (مختار الصحاح) للشيخ الأمام الرازى - مكتبة لبنان - لبنان - ط ١٩٨٦ - باب ط - ص١٦٧.

(٤) د/ هلالى عبد اللاه أحمد - قانون العقوبات وأزمة الحاسبات - مرجع سابق - ص ٨٣.

(٥) يراجع فى ذلك: (لسان العرب) لمحمد بن بكرين منظور - دار المعارف - جـ ٤ - ص ٢٧٠٢، (أساس البلاغة) لأبى القاسم محمود بن عمر الزمخشرى - دار صادر - بيروت - لبنان - ص ٣٩٥.

وجاء في المورد: أن الفعل Embed في اللغة الانجليزية، يقابله في اللغة العربية يطمر أو يجعله جزءاً لا يتجزأ، وأن المصدر Embedded يقابله في اللغة العربية مطمور.

وجاء في المنهل[1]: أن الفعل Inclure في اللغة الفرنسية يقابله في اللغة العربية احتوى، اشتمل، أدرج، أرفق، ضمن. وأن الصفة Inclus يقابلها في اللغة العربية مُندرج، مرفق بـ، مرفق طيه، ضمنه، داخل، ضمني، طي.

ومن ذلك نخلص إلى أنه يقصد بالنظم المطمورة لغة: تلك النظم المخبأة أو المخفاة أو المدفونة أو المدرجة أو المدمجة في معدة من المعدات، أو آلة من الآلات، بحيث تصبح جزءاً لا يتجزأ منها[2].

وفي الأصطلاح: لا يختلف معنى النظم المطمورة كثيراً عما سبق ذكره لغة(*)، إذ يقصد بالنظام المطمور أي نظام أو وسيلة تحتوي على معالج دقيق Microprocessor أو جهاز تحكم دقيق Microcontrollen (**)من أجل أداء خدمة أو وظيفة معينة[3]. فالنظم المطمورة مبرمجة لأداء منظومة ثابتة من المهام[4].

(١) منير البعلبكي – (المورد.. قاموس انجليزي/عربي) – بيروت – دار العلم للملايين – ط ٣٢ – سنة ١٩٩٨ – ص ٣٠٩.

(٢) د/ هلالي عبد اللاه أحمد – المرجع السابق – ص ٨٣.

(*) يختلف النظام المطمور Embedded عن الحاسب الشخصي (P.C) من حيث إن النظام المطمور ليس له شاشة عرض Monitor أو لوحة مفاتيح eyboardK كقاعدة عامة. ويرد على هذه القاعدة بعض الاستثناءات، التي منها آلة أو ماكينة النقود الآلية (A.T.M) التي تتكون من شاشة عرض ونوع معين من أنواع المفاتيح لإدخال الأوامر. (المرجع السابق مشيراً إلى:

- Gregory (Corinne): "Assessing your Embedded system", the Millennium Jouranal, vol - V-VI, June, 1998, p. I.

(**) المعالج الدقيق هو وحدة التشغيل المركزية (C.P.U.) والتي تتكون من وحدة الحساب والمنطق (A.L.U)، ووحدة التحكم (C.U.) موضوعة على شريحة واحدة Chip. يراجع: د/ محمد فهمي طلبة وآخرون – مرجع سابق – ص ٣٠٢، ٣٠٣.

(3) Gregory (corinne): Art, cit. p. 1

(4) Ibid.

كما عُرفت النظم المطمورة: بأنها عبارة عن وسيلة تستخدم فى التحكم أو فى مراقبة أو مساعدة تشغيل معدة أو آلة أو مصنع، بحيث تصبح جزءاً لا يتجزأ منها. وهى تتكون من معالج دقيق أو جهاز تحكم دقيق أو دوائر متكاملة ذات تطبيق خاص[١]، Application specific Integrated circuit (A.S.I.S).

**• ثانياً: المكونات الداخلية للنظم المطمورة:**

تعتمد النظم المطمورة على شرائح إليكترونية متناهية فى الصغر تسمى Micro Chips، وهى عبارة عن دوائر إليكترونية يتم تثبيتها على شريحة من السليكون[٢]، وبها مسارات عبارة عن طبقات معدنية رقيقة جداً تعمل كأسلاك ويمكن استعمال هذه الشريحة فى الذاكرة الرئيسية Main Memory أو فى وحدة المعالجة المركزية C.P.U[٣]. وتعمل هذه الشرائح على تحويل التيار الكهربائى إلى نبضات أو إشارات فائقة الدقة فى انتظامها. وهو ما يعد أساس عملها فى تنفيذ العمليات الحسابية وإدارة الدوائر الإليكترونية والتحكم فى تشغيلها بانتظام فائق الدقة. لذلك كان أول تطبيقات هذه الشرائح هو استخدامها فى تشغيل الساعة الداخلية بالمعالج Real Time Clock (R.T.C.) وحساب الوقت بدقة وصلت إلى جزء من المليون من الثانية الواحدة[٤].

**• ثالثاً: أقسام النظم المطمورة من حيث البساطة والتعقيد:**

وتنقسم النظم المطمورة من حيث البساطة والتعقيد إلى نوعين رئيسين[٥]،

---

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٨٣.

(2) Frautschi (Mark. A.): "Embedded Systems and The Year 2000, Proble:m", department of Phyaics and Astronomy, Johns Hopkins, U.S.A. Verion of 22 may, 1998, p. 1.

(٣) د/ محمد فهمى طلبة وآخرون: «الموسوعة الشاملة لمصطلحات الحاسب الاليكترونى» المرجع السابق، ص ٩٤.

(٤) سامى شلبى، المرجع السابق، ص ٢٣.

(5) Gregory (Corinne): Art. Cit. p. 1.

الأول: النموذج البسيط للنظام المطمور A typical, simple embedded System ويتكون من حاسب صغير Microcmputer ذى لوحة دوائر إليكترونية أحادية Singleboars مع كيان منطقى Software ذى ذاكرة قراءة فقط Read only Memory (ROM) وبرنامج تطبيقى ذى غرض معين يبدأ العمل بمجرد التشغيل ولا يتوقف حتى يتم غلق النظام.

أما النوع الثانى: فهو النموذج المركب للنظام المطمور A typical Complex Embedded System الذى يتكون من عدة أنظمة بسيطة تعمل معاً لأداء مجموعة جوهرية من احتياجات أكبر. ومن ذلك على سبيل المثال عربات النوم الأوتوماتيكية وخطوط الإنتاج فى المصانع.

- **رابعاً: الاستخدامات والتطبيقات للنظم المطمورة:**

وتستخدم النظم المطمورة فى العديد من التطبيقات الإنتاجية والتى يمكن بلورتها على النحو التالى(١):

- **الأدوات المنزلية Household Items:**

- أجهزة الفيديو Video، أجهزة الميكروويف Microwaves، نظم الأمن المنزلية Home Security System، آلات الرد على التليفون Telephone Answering Machines.

- **النظم المكتبية Office Systems:**

- أجهزة أو نظم البريد الصوتى Voicemail system، أجهزة الفاكس Faxs، آلات النسخ Cop-iers.

---

(١) راجع فى هذا الشأن:

- Gregory (Corinne): Art. Cit., pp. 2-3.

مشار إليه لدى: د/ هلالى عبد اللاه أحمد - مرجع سابق - ص ٨٥.

• نظم المباني Building Systems:

– أجهزة الإضاءة والمولدات Backup Lighting and generators، أجهزة التدفئة والتهوية وتكييف الهواء Heating, Ventilation, and air Conditioning (HVAC)، المصاعد والسلالم الميكانيكية Elevators and escalators، نظم الأمن Security Systems، أقفال الأبواب Door Locks.

• نظم المرافق والتصنيع Utility and Manufacturing Systems:

– أجهزة التصنيع Manufaturing Plants، نظم المياه والصرف الصحى Water and Sewage Systems، محطات توليد الطاقة Power Stations، نظم شبكات الطاقة Power Grid Systems، أنظمة تكرير البترول Oil Refineries، خطوط الإنتاج الآلية Automated Factories، نظم التحكم فى الطاقة Energy Control Systems.

• المواصلات والاتصالات Transportation and Communiations:

– الكترونيات الطيران Avionics، نظم المراقبة الجوية Air Traffic Control Systems، القطارات Trains، الأوتوبيسات Buses، وسائل النقل البحرى Ferries، السيارات الخاصة Cars، إشارات المرور Traffic Lights، نظم الرادار Radar Systems(*)، آلات قطع التذاكر Ticketing Machines، التليفونات Telephone، نظم الكابلات Cable Systems، الأقمار الصناعية وأجهزة النظام العالمى للاستقبال Satellites and Global Positioning System Devices(**).

---

(*) كلمة رادار RADAR هى الحروف الأولى من المصطلح الانجليزى: Radio Detection And Ranging بمعنى «الكشف وتحديد الموقع بالراديو». فترسل موجات الراديو على شكل حزمة رفيعة من جهاز إرسال فترتد ثانية من أى جسم تصطدم به فى طريقها. ويقوم جهاز استقبال بالتقاط الأصداء، وتظهر صور للمنظر فوق ما يشبه شاشة التليفزيون. وتبدو نبضات الرادار كالنقط الصغيرة.

(**) يستخدم القمر الصناعى Satellite فى نقل البيانات والصور بين النظم المختلفة. وهو يعمل كعاكس للإشارة الصادرة من نقطة معينة على الأرض، وإعادتها إلى نقطة أخرى على سطح

–/–

• البنوك والمال Banking and finance:

– ماكينات النقود الآلية(ATM) Automatic Teller Machine (*)، ماكينات التعامل مع بطاقات الائتمان Credit Card Piont of Sale Machines.

• النظم الطبية Medical Systems:

– أجهزة تنظيم ضربات القلب Heart defibrillators(**)، نظم معلومات المرضى Patient information systems، نظم مراقبة المرضى Patient monitoring Systems، مراقبة الأدوية Pharmaceutical control.

---

= الأرض. والقمر الصناعى يكون تقريباً ثابتاً بالنسبة للإشارات الموجبة الدقيقة Microwave Signals لأنه يكون موضوعاً على بعد حوالى ٢٢٣٠٠ ميل عن سطح الأرض ويدور فى مسار دائرى بنفس سرعة دوران الأرض. والقمر الصناعى يساعد على نقل البيانات من أى مكان على الأرض إلى عدة أماكن متفرقة فى نفس الوقت. كما يستخدم الاصطلاح Satellite Computer للدلالة على حاسب تابع ومتصل بحاسب أكبر منه. راجع: د/ محمد فهمى طلبه وآخرون: «الموسوعة الشاملة لمصطلحات الحاسب الإليكترونى»، مرجع سابق، ص ٣٣٩.

(*) ماكينات النقود الآلية عبارة عن أجهزة يتم توزيعها فى أماكن متفرقة من المدينة مع ربطها بحاسب مركزى. وهى تمكن عملاء البنك من إيداع الأموال أو سحبها أو نقل أرصدتهم فى البنك من فرع إلى آخر. ويقوم الحاسب فى نهاية اليوم مثلاً بإدخال كل التعديلات الخاصة بالسحب والإيداع دفعة واحدة عن طريق ملف الحركة الخاصة به Transaction File، ويتم ذلك عن طريق كروت بلاستيك تسلم لكل عميل. وتتم كتابة رقم الحساب فى هذه الكروت. وعند إدخال أحد الكروت فى هذا الجهاز يتم قراءة بياناته ونقلها إلى المعالج الذى يقوم بمعالجة الحساب الخاص بهذا العميل والتأكد من أن رصيده يغطى المبلغ المطلوب سحبه مثلاً. راجع: د/ محمد فهى طلبة وآخرون: المرجع السابق، ص ٤٤ – ٤٥.

(**) فى الظروف الطبيعية، فإن منظم ضربات القلب الطبيعى فى القلب والموجود فى أذين القلب يعطى نبضات كهربائية والتى تنتقل خلال النظام العصبى الداخلى للقلب إلى البطين والذى يمكن أن يتقلص لإعطاء عمل الضخ المطلوب. وفشل النظام العصبى Heart Block ينتج فى إبطاء أو توقف Cessation ضربة القلب وعدم سريان كاف. ولذا كانت الحاجة إلى نبضات كهربائية تحفز انقبضات البطين. وقد تم الحصول على هذه النتيجة عن طريق دوائر اليكترونية مدمجة تعمل على تنبيه البطين على الانقباض إذا أبطأ أو توقف. راجع: م/ فاروق سيد حسين: «استخدام الوسائل الإليكترونية فى الطب» بيروت، دار الراتب الجامعية، ١٩٩٣، ص ٢٦–٢٧.

• الأهمية في استعراض النظم المطموردة:

تعزى أهمية النظم المطمورة إلى سعة انتشارها. إذ يبلغ مجموع الأنظمة المطمورة على مستوى العالم مع نهاية هذا القرن خمسين بليون نظام 50 Billion embedded Systems(١).

فمع توالى فيض الاختراعات المترتبة على هذه الإليكترونيات «أصبحنا نعتمد بشكل متزايد على هذه الرقائق المطمورة فى كل شئ بدءاً من الترمومستات Thermostat وحتى أجهزة اكتشاف الدخان على أسطح المبانى.

بالإضافة إلى أن هناك العديد من استخدامات النظم المطمورة يرتبط ارتباطاً مباشراً بحياة الإنسان، وخاصة فيما يطلق عليه تسمية النظم الحرجة Critical Systems. ومثال ذلك، الرقائق المطمورة فى الآلات والمعدات الإليكترونية المستخدمة فى المستشفيات، وأجهزة قيادة الطائرات، وكذلك الرقائق التى تراقب إليكترونياً عمليات إنتاج وتحليل المواد النووية(٢) Nuclear Materials.

كما تعزى أخيراً الأهمية الفائقة للنظم المطمورة، إلى الصعوبة الفنية فى التعامل معها، وذلك يرجع إلى وجود الشرائح الإليكترونية ضمن التركيب الداخلى لها Digital Control Clocks فى أماكن غير ظاهرة للأعين(٣).

ورغم ذلك فإنه ترتفع نسبة ممارسة النشاط الإجرامى والممارسات غير المشروعة التى تستهدف الأنظمة المطمورة، ويفرز لنا ذلك جرائم مطمورة، هى أحد أوجه جرائم المعلوماتية.

---

(١) راجع فى هذا الخصوص: - FRAUTSCHI (Mark a.): Art. cit., p. 1,

(٢) لمزيد من الاستفاضة حول استخدامات الطاقة النووية راجع على وجه الخصوص:

– د/ ميرفت محمد البارودى: «المسئولية الجنائية للاستخدامات السلمية للطاقة النووية» رسالة دكتوراه – كلية الحقوق – جامعة عين شمس، سنة ١٩٩٣.

(٣) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٨٩.

## الفرع الثاني

## الإنترنت (INTERNET)

تعتبر شبكة الاتصالات الدولية (INTERNET) – والتى ربطت بين الملايين من أجهزة الحاسب الآلى على مستوى العالم، حتى أصبحت كافة التعاملات سواء كانت معلومات أو أموال تتم من خلالها – من أهم التطورات التكنولوچية فى تاريخ البشرية، وهى تعتبر أضخم شبكة كمبيوتر على مستوى العالم، وهى ثمرة الاندماج بين تكنولوجيا الحاسب وتكنولوجيا الاتصالات لأن شبكة الإنترنت استطاعت أن تصل المراكز بالفروع بالرغم مما بينهما من مسافات.

وقد بدأت جذور شبكة الإنترنت عام ١٩٦٩ حينما أنشئت شبكة (ARPA NET) التى أنشأتها وكالة مشاريع الأبحاث المتقدمة (ARPA)(*) التابعة لوزارة الدفاع الأمريكية (بنتاجون)، وكان الهدف الأساسى منها هو تأمين تبادل المعلومات العسكرية بالغة السرية والحيوية بالنسبة للأمن القومى الأمريكى(١).

ومع بداية حقبة السبعينات وبانضمام وكالة الفضاء الأمريكية (NASA) والمؤسسة القومية للعلوم ومراكز البحث العلمى، أخذت الشبكة الطابع المدنى وأصبح التمويل الخاص بها يتم عن طريق جهات حكومية، وبانضمام أعداد هائلة من الشبكات الخاصة بالشركات والمؤسسات، أخذت الشبكة الطابع التجارى بعد أن كانت مقتصرة على الجوانب الأكاديمية والعسكرية فقط(٢).

---

(*) كلمة (ARPA) هى اختصار لعبارة:

(Advanced Researching Projects Agency)

(١) هيثم نيازى وهبى – رحلة عبر الشبكة الدولية الإنترنت – الحسينى لنظم المعلومات – القاهرة، سنة ١٩٩٦، ص ٢١.

(٢) د/ يحيى مصطفى حلمى وآخرون – أساسيات الحاسبات الإلكترونية – مكتبة عين شمس – القاهرة – سنة ١٩٩٥، ص ٥.

البند الأول: تطور شبكة الإنترنت[1]:

صممت شبكة ARPANEI من أجل دعم الأبحاث العلمية وهى تعد الجزء الأول لشبكة الإنترنت وقد تكون النموذج الأول لهذه الشبكة من أربعة أجهزة حاسبات موزعة كالآتى:

١- جامعات يوتاه.

٢- كاليفورنيا فى سانتا باربرا.

٣- كاليفورنيا فى لوس أنجلوس.

٤- معهد ستانفورد الدولى للأبحاث.

نتيجة لهذا الوضع فإن شبكة الـ Arpanet قد نمت بشكل ملحوظ، والشبكة التى كانت بسيطة تحولت إلى نظام اتصالات فعال، وفى ذلك الوقت كانت الشبكة قاصرة على الجيش والجامعات والباحثين، ونتيجة لهذا الوضع فلقد أصبحت Arpanet عبارة عن شبكة تتكون من شبكات ذات أطراف متعددة، وترسل المعلومات فيها باستخدام تقنية تفتيتها إلى مجموعات من الحزم الصغيرة Pockets، تتحرك بحرية واستغلالية من طرف إلى آخر لتصل إلى مبتغيها.

وفى عام ١٩٨٣م ونتيجة لنجاح المشروع.. رأت وزارة الدفاع الأمريكى فصل الشق العسكرى Mil Net عن الشبكة،ومنذ عام ١٩٨٠م فإن شبكات عديدة تكونت لخدمة بعض الفئات والمنظمات إحدى هذه الشبكات كانت للمجتمعات الأكاديمية وأخرى لمنظمات أبحاث الكمبيوتر حيث وصلت الباحثين بعضهم ببعض ليتشاركوا فى المعلومات وفى عام ١٩٨٦ فإن مؤسسة العلوم الوطنية National Science Foundation قامت بإنشاء شبكة NSFNET عن طريق توصيل خمسة حاسبات رئيسية عملاقة وذلك لخدمة مركز البحوث الأمريكية بحيث حلت هذه الحسابات والتى تعمل بسرعة فائقة محل النظام السابق.

---

(١) حسن مدحت الروبى وآخرون – الجرائم المرتكبة عبر شبكة المعلومات الدولية ومواجهتها – بحث مقدم فى فرقة القيادات الأمنية – الدورة ١١٣ – معهد القادة – كلية التدريب والتنمية – أكاديمية الشرطة، فبراير ٢٠٠٧ – ص ٣ وما بعدها.

واعتباراً من عام ١٩٨٧م تزايدت أعداد المتعاملين مع هذه الشبكة، وخصوصاً بعد السماح للأفراد العاديين باستعمالها، حتى أصبحت شبكة الإنترنت الآن أكبر شبكة فى تاريخ البشرية.

وفى عام ١٩٩٧م قدر عدد مستخدمى شبكة الانترنت بما يقرب من ١٦ مليون مستخدم زاد إلى الخمسين مليون عام ١٩٩٨م وفى نهاية عام ٢٠٠٢م وصل عدد مستخدمى شبكة الإنترنت لما يقرب من ٦٥٥ مليون شخص.

**الجيل الثاني للإنترنت:**

بدأ الجيل الثانى بالظهور على أرض الواقع ويتمثل ذلك فى عدة مشاريع منها:

– الإنترنت (Internet) وإنترنت الجيل المقبل NGI - Next Generation Internet وشبكة Cant ويعتبر هذا الجيل نسخة مطورة من بروتوكول IPV كما يدعم ميزتين مهمتين همـا: الإرسال المتزامن المتعدد الوجهات، وميزة جودة الخدمات التى تدعم البحث الحى لملفات الفيديو وتدعم تطبيقات الوسائط المتعددة (Multimedia).

وتعمل حالياً أكثر من ١٧٠ جامعة على تطوير وتنفيذ ما تتطلبه شبكة الانترنت من تطبيقات وتقنيات شبكية متقدمة، وذلك بالاشتراك مع الحكومة الأمريكية ومع أكثر من ٦٠ شركة رائدة عالمياً فى قطاع تكنولوجيا المعلومات.. ولن تقتصر استخدامات هذه التطبيقات والتقنيات على الأبحاث والتعليم، بل ستشمل أيضاً أغراضاً تجارية.

وجدير بالذكر أن إنترنت 3 ليست منفصلة عن الإنترنت ولن تكون بديلا عنها، وقد أصبح العمود الفقرى لإنترنت 3 يتكون من ألياف ضوئية (Fiber Optical) فعالا (Live) عام ١٩٩٩م، وسوف تؤدى إنترنت 3 إلى تسريع نشر التطبيقات والخدمات الشبكية إلى المزيد من جهود الإنترنت، كما ستشجع تطوير تطبيقات ثورية للإنترنت.

### الجيل الثالث للإنترنت:

من المتوقع أن يدعم جميع المزايا المتقدمة ولاسيما تلك التى تتطلب سرعة عالية جداً ومن أبرز المشاريع المقدمة شبكة Canet 3 وشبكة Super Net ويدعم هذا الجيل ميزتين مهمتين هما:

- استخدام تقنية: وهى تقنية تستخدم الألياف الضوئية فى الإرسال بسرعات تصل إلى ٤٠٠ ميجابت/ثانية مما يسرع نقل الصوت والفيديو بدرجة هائلة.
- استغلال الألياف المعتمة فى التحويل والتوجيه.

وفى حقيقة الأمر فإن الألياف المعتمة هى:مصطلح يتعلق بالألياف الضوئية وقدرات عالية لم يتم استغلالها حتى الآن.

### البند الثاني: تعريف الإنترنت وأنظمة اتصالاته:

### أولاً: تعريف الإنترنت:

الإنترنت هى تلك الشبكة (العنكبوتية) التى تربط بين كم هائل من الحاسبات، مستعملة فى عملية الربط هذه مختلف وسائل الاتصالات السلكية واللاسلكية، مثل الخطوط الهاتفية العامة أو الخطوط الخاصة (Private Circuits) أو الأقمار الصناعية أو الكيابل والألياف البصرية (Fiberoptic) وغيرها من وسائل الاتصالات الحديثة وفائقة السرعة. وتمتد هذه الشبكة حول العالم لتؤلف شبكة دولية هائلة لتبادل المعلومات، بحيث يمكن لمستعملها الدخول إليها فى أى وقت ومن أى مكان فى العالم ولو كان فى الفضاء، على أن يكون معه حاسوب مجهز بوسائط الاتصال بالشبكة لتلقى وارسال البيانات عبر مزود الخدمة (Service Provider)[1].

---

(١) د/ محمود عبد الرحيم الديب – الحماية القانونية للملكية الفكرية (فى مجال الحاسب الآلى و الانترنت) – بحث منشور بمجلة البحوث الفقهية والقانون – كلية الشرعية والقانون – جامعة الأزهر – فرع دمنهور – العدد ١٨ – جـ١ – ١٤٢٤هـ، ٢٠٠٣م – ص ٣٩٠.

فشبكة الإنترنت إذن هى شبكة هائلة من أجهزة الكمبيوتر المتصلة فيما بينها بواسطة خطوط الإتصال عبر العالم، وعلى الرغم من أن الاتصال عبر الانترنت يتم عبر الخط الهاتفى، إلا أنها منفصلة كلياً عن النظام الهاتفى، فلا يتحمل مستخدم الانترنت تكلفة الاتصال الدولى كما هو الحال بشأن الاتصال الهاتفى الدولى، فالأمر لا يعدو أن يكون مجاناً، مقارنة بالاتصال الهاتفي الدولى، ولا يعنى ذلك أن استخدام الانترنت مجانى تماماً، بل إنه يجب على مستخدم هذه الشبكة أن يدفع مقابلاً إلى مقدم خدمة الانترنت نظير قيامه بتقديم هذه الخدمة(١).

وتتميز خدمة الانترنت عن الخدمات الاعلامية التقليدية بالكم الهائل المتبادل من المعلومات بسهولة ودقة وسرعة فائقة. ويتم ذلك عبر إحدى النظامين للشبكة وهما نظم الشبكات المحلية، وهو نظام مغلق يربط بين مجموعة من الحاسبات داخل منطقة محلية معينة (LAN Local Area Network). ونظام الشبكة الدولية التى تربط بين عدة شبكات فى إطار واحد، مستخدمة فى ذلك مختلف وسائل الاتصالات السلكية واللاسلكية (WAN Wide Area Network).

فالإنترنت هى شبكة اتصالات دولية متصلة بشبكات المعلوماتية الدولية فى أنحاء العالم وبنوك المعلومات ومراكز البحث العلمي والمكتبات العالمية والجامعات والمستشفيات وبمختلف مصادر المعلومات الأخرى والدوائر الحكومية وغيرها، فى عالم متشابك ومتداخل لا تعرف له نهاية ولا بداية. فهو عبارة عن سوق يعرض فيه كل ما تنتجه البشرية. وسوف نتعرض لبروتوكول الاتصال عبر الإنترنت، ولبعض مجالات استعمال الانترنت.

---

(١) د/ أسامة أبو الحسن مجاهد – خصوصية التعاقد عبر الإنترنت – دار النهضة العربية – سنة ٢٠٠٠ – ص ٦.

• وعلي ذلك يمكن تعريف شبكة (INTER NET) بانها[1]،

- «شبكة تربط شبكات الحاسب الآلى على مستوى العالم، عن طريق بروتوكولات تحكم عملية المشاركة فى تبادل المعلومات، وأيضاً بروتوكولات تضبط عملية التراسل، وهذا ما جعل كثيراً من الجهات تكون هدفاً لإرتكاب الجرائم من جانب مرتكبيها».

**ثانياً: بروتوكولات الأتصال بشبكة الأنترنت:**

يتحكم فى عملية التراسل عبر شبكة الإنترنت مجموعة من بروتوكولات التراسل(*)، وأشهر هذه البروتوكولات.. بروتوكول (TCP / IP)[2] ويعمل نظام (TCP) من خلال أربعة مستويات (Layers) خاصة بالتطبيقات والاتصال والتشبيك والولوج، حيث يقوم النظام بتقسيم الرسائل المرسلة عبر الشبكة إلى حزم (Packets)، وكل حزمة يتم تمييزها برقم معين وعنوان الوصول، ثم يتم إرسال هذه الحزم خلال الشبكة حيث تبدأ مهمة النظام (IP) حيث ينقل هذه الحزم إلى الحاسب الآخر، وفى الحاسب الآخر يقوم الـ (TCP) باستقبال هذه الحزم ويختبر وجود أى أخطاء بها، وإذا وجد خطأ فإنه يطلب إعادة إرسال الحزمة المحتوية على هذا الخطأ، ويقوم (TCP) بعد ذلك باستخدام أرقام الحزم فى إعادة بناء الرسالة الأصلية.

ويمكن القول أن وظيفة (IP) هى نقل البيانات الخام (الحزم) من مكان إلى آخر ووظيفة الـ (TCP) هى تقسيم البيانات المرسلة إلى حزم وتجميعها والتأكد من خلوها من الأخطاء.

---

(١) أيمن عبد الحافظ - المخاطر التى تتعرض لها شبكة الإنترنت وسبل حمايتها - مجلة مركز بحوث الشرطة - العدد ٢٢ - يوليو ٢٠٠٢ - ص ٤٣١.

(*) البروتوكول: هو مجموعة من القواعد التى تقدم توصيفاً فنياً لكيفية تنفيذ شئ ما. فمثلاً يوجد بروتوكول يصف بدقة الهيئة التى يجب كتابة الرسائل بها.

(٢) بروتوكول (TCP / IP) هو اختصار لعبارة:

(Transmission Control Protocol / Internet Protocol)

وفوائد استخدام الحزم عديدة فهى تسمح للإنترنت باستخدام نفس خطوط الاتصال من جانب العديد من المستخدمين فى ذات الوقت، ونظراً لأن الحزم لا تتحرك مع بعضها فإن خط الأتصال يستطيع نقل أنواع مختلفة من الحزم من مكان إلى آخر.

كذلك عند وقوع أى خطأ فى أحد الحزم يمكن إصلاحه عن طريق إعادة نقل هذه الحزمة وليس الرسالة كلها، وهذا يؤدى إلى زيادة سرعة الشبكة فى عملية تبادل المعلومات.

- **طرق الاتصال بشبكة الإنترنت:**

يمكن الاتصال بشبكة الإنترنت بطريق مباشر أو بطريق غير مباشر.

**- الاتصال المباشر بشبكة الإنترنت:**

أ – يتم ذلك من خلال كابلات توصيل (Cables)، ويتميز هذا النظام بسهولة الدخول إلى الشبكة، لكن رغم ذلك فإنه لا يتيح مرونة كاملة للمستخدم فى حالة الرغبة فى نقل الحاسب إلى مكان آخر، حيث يعنى ذلك أن يتم مد خطوط الكابلات إلى المكان الجديد.

ب– باستخدام الآلياف البصرية.

ويلاحظ أن الألياف البصرية لا يتجاوز سمك السلك فيها ٠,٠١ سم أى سمك شعرة رأس الإنسان، ولكن نظرياً يستطيع هذا السلك نقل خمسين مليون محادثة هاتفية فى وقت واحد وبسرعة الضوء(*).

---

(*) طريقة عمل الألياف البصرية شبيهة جداً من الناحية النظرية بطريقة عمل الشبكات الهاتفية بالأسلاك النحاسية أو الشبكات البرقية، وذلك من خلال قيام الشبكات البرقية بترجمة النبضات الكهربائية إلى أشارات من لغة مورس (Morse) التى يجرى تحويلها إلى اللغة المتداولة، وفى أنظمة الاتصالات البعدية فإنها تتولى نقل نبضات ضوئية بدلاً من النبضات الكهربائية. للمزيد يراجع: مقالة (ألياف بصرية لزيادة سرعة الإنترنت – مجلة لغة العصر – العدد ٨ – أغسطس ٢٠٠١ – ص ٤٧.

- **الاتصال غير المباشر بشبكة الانترنت (الاتصال التليفوني):**

حيث يسمى الاتصال غير المباشر بالشبكة بـ (الأتصال التليفونى) ، ويتميز بالمرونة لأنه يتيح للمستخدم إمكانية نقل الجهاز إلى أى مكان شريطة وجود خط تليفونى، وكل ما يحتاجه الجهاز لتوافر تلك الإمكانية هو جهاز (Modula Tor) لكى يقوم بتحويل إشارات الحاسب (Computer Signals) وهى أشارات رقمية (Digtal) إلى إشارات التليفون (Telephone signals) وهى إشارات تناظرية (Analog)(*) .

(*) أما الجهاز الذى يحول الإشارات التناظرية إلى الاشارات الرقمية يسمى الموائم العسكى (Demodulator)، ولذلك فإن الأتصال بشبكة الانترنت يحتاج إلى الجهازين السابقين واختصاراً يطلق عليهم (Modem) وهى اختصار Modulatar de modulator.

**البند الثالث: خصائص شبكة الإنترنت[1]:**

مجموعة من الخصائص تميز نظم المعلوماتية المتداولة من خلال الإنترنت.

**١- اللامكان:**

تتخطى شبكة الإنترنت كل الحواجز الجغرافية والمكانية التى حالت منذ فجر التاريخ دون انتشار الأفكار وامتزاج الناس وتبادل المعارف، ومعلوم أن حواجز الجغرافيا منها اقتصادى كتكلفة شحن المواد المطبوعة من مكان إلى آخر، ومنها سياسى (حيلولة بعض الدول دون دخول أفكار وثقافات معينة إلى بلادها)، أما اليوم يمر كم هائل من المعلومات عبر الحدود على شكل إشارات إلكترونية لا يقف فى وجهها شئ، ويترتب على هذا كثير من إيجابيات وسلبيات لابد من الانتباه إليها.

**٢- اللازمان:**

إن السرعة الكبيرة التى يتم بها نقل المعومات عبر الشبكة تسقط عامل الزمن من الحسابات، وتجعل المعلومة فى اليد حال صدورها، وتسوى بين كل أبناء البشر فى حق الحصول على المعلومة فى نفس الوقت، وبالتالى فنحن نعيش فى عصر «المساواة المعلوماتية».

**٣- التفاعلية:**

تعودت وسائل الإعلام التقليدية أن تتعامل مع الفرد كجهة مستقبلة فقط، ينحصر دوره فى أخذ ما يعطونه وفقد ما لا يعطونه، ولذلك فهم الذين يقررون ما نقرأ أو تسمع أو تشاهد، أما فى عصر ا لإنترنت فالفرد الذى يقرر ماذا ومتى ما يريد أن يحصل عليه من معلومات، وأكثر من ذلك فبالإمكان من خلال منتديات التفاعل والحوار الإنتقال من دور المستقبل إلى دور المرسل أو الناشر،

(١) د/ محمد أبو زيد محمد على – بحث (الجداول الإنتخابية ونظم املعلومات) – مجلة كلية الدراسات العليا – أكاديمية الشرطة – القاهرة – العدد ١٣ – يوليو ٢٠٠٥. – ص ٦٨.

وهذه نقلة تحدث لأول مرة، وتمكن الناس من التحرك على أرض مستوية دون أن يطغى صوت أحدهم على الآخر.

**٤- المجانية:**

أو بصورة أدق – شبه مجانية – وهو أمر لم يحدث تماماً بعد، لكنه سيحدث خلال السنوات القادمة، حيث إن الكثير من الأنماط التجارية بدأت تتبلور، لتمكن المجتمع من اعتبار خدمة الإنترنت من الخدمات الأساسية فى الحياة، والتى سيتم توفيرها للمجتمع بشكل مجانى أو شبه مجاني، ومعروف اليوم أنه بالإمكان أن يتم الاتصال بالانترنت ٢٤ ساعة يومياً مقابل مبلغ زهيد شهرياً.

**٥- الربط الدائم:**

مع تطور التقنيات التى تمكن من الاتصال بالإنترنت لم تعد بالضرورة الاقتصار على استخدامها من الحاسب الشخصى فى العمل أو المنزل بل أصبح بإمكان الفرد أن يتصل بالشبكة من طائفة كبيرة ومتنوعه من الأدوات، كحاسبات الجيب والهواتف النقالة، وبذلك، سيكون على ارتباط دائم بالإنترنت فى كل مكان وزمان، يتابع الأخبار ويتسوق ويستدعى المعلومات المهمة فى الوقت المناسب.

**٦- السهولة:**

لا يحتاج المرء أن يكون خبيراً معلوماتياً أو مبرمجاً حتى يستخدم الإنترنت، فبإمكان الصغير السن، والشيخ ذى السبعين عاماً أن يستخدما الإنترنت بسهولة ويسير، ولا يحتاج رواد الشبكة إلى تدريبات معقدة للبدء فى استخدامها، بل الأمر يحتاج إلى مجرد مقدمة فى جلسة لمدة ساعة مع صديق لتوضيح المبادئ الأولية للاستخدام(١).

---

(١) راجع: العميد/ نجاح فوزى – ورقة عمل بعنوان: الانعكاسات السلبية لاستخدام الانترنت فى ارتكاب الأنشطة الإجرامية المستخدمة فى مجال المخدرات، مقدمة إلى ندوة الأمن والإنترنت، مركز بحوث الشرطة، ١٥ يونيه ٢٠٠٣، ص ص ٦ – ٧.

**البند الرابع: مجالات استعمال الإنترنت[1]:**

لقد انطلقت شبكة الإنترنت كوسيلة للبحث العلمي، حيث قامت بالربط بين مجموعة من العلماء لتبادل نتائج بحوثهم وتوفير أمن الاتصال بين مختلف أجهزة الدفاع الأمريكية في حالة نشوب حرب نووية، ثم تطورت هذه الفكرة وانتشرت لتشمل المجال العلمي البحت ومجال الدفاع والأمن القومي. ومع التطور التكنولوجي ازداد مجال استعمال الإنترنت ليشمل جميع مجالات الحياة البشرية من علوم وتجارة واقتصاد وتبادل للفنون بمختلف أنواعها والملفات والمعلومات، وامتدت كأي نشاط بشري ليشمل الجريمة المنظمة والدعارة، والأفلام الإباحية وقرصنة حقوق المؤلفين الأدبية، وعمليات التجسس والإرهاب وغيرها من الجرائم والانحرافات البشرية، ولكن رغم كل هذا فإن شبكة الانترنت ما تزال تقدم خدمات رائدة للبشرية نذكر منها ما يلي:

- **خدمة البريد الإلكتروني** Electronic Mail (e-mail): يستطيع المشترك في هذه الخدمة عبر المشغل Service provider أن يرسل ويستقبل ما شاء من الرسائل والمعلومات إلى من يشاء وحيثما كان الطرف الثاني قريباً أو بعيداً على الطرف الآخر من الكون، وفي أي وقت أراد، وذلك في كنف السرية والخصوصية التامة، حيث يوجد لكل مستخدم كلمة سر خاصة به تمكنه من الدخول واستعمال بريده الالكتروني دون غيره.
- **استخدامات أجهزة العدالة الجنائية:** لقد انتشر استعمال الحاسوب لمحاربة الإرهاب وتجارة المخدرات والجريمة المنظمة وغيرها من الجرائم، وذلك بالاحتفاظ بملفات المجرمين وجميع بياناتهم وتحركاتهم. حيث يتم الكشف على المجرم بالصورة والمعلومات في وقت قياسي. واستخدمت الدول المتقدمة مثل ألمانيا وفرنسا وبريطانيا والولايات المتحدة الأمريكية شبكة

---

(١) د/ جميل عبد الباقي الصغير – الإنترنت والقانون الجنائي – الأحكام الموضوعية المتعلقة بالإنترنت، دار الفكر العربي، القاهرة، ٢٠٠١، ص ١٢ وما بعدها.

الإنترنت في عرض صور المجرمين والمشتبه فيهم لحث الجماهير على الإبلاغ عنهم بالإتصال بالإنتربول عبر الإنترنت.

- **الإطلاع على أخبار العالم:** تتيح شبكة الانترنت مواقع متخصصة لبث الأخبار العالمية والمحلية حسب اختيار المستعمل، وتشمل الأخبار السياسية والرياضية والفنون بمختلف أنواعها، والحرب والسلم والأخبار العلمية المتخصصة والاقتصاد وآخر أخبار البورصة المحلية منها والعالمية. وأشهر القنوات الفضائية كالجزيرة بدولة قطر و...CNN, BBC, MBC ART وبإمكان مستخدم الشبكة تصفح أهم عناوين صحف العالم والمجالات المتخصصة والجديد من المستشفيات العلمية.
- **التجارة الإلكترونية (E-commerce):** فمن خلال شبكة الإنترنت يمكنك البيع والشراء دون أن تنتقل من منزلك أو مكتب، وذلك بتمرير أمر الشراء والدفع مستعملاً الإنترنت والحساب الالكتروني باستعمال بطاقة الإئتمان (Visa Card) مع ملاحظة أن هذا النوع من التجارة لم يصل للمستوى المتوقع، نسبة لتخوف العميل من سوء استخدام بطاقة الإئتمان البنكية من قبل الغير(١). ومع ذلك فقد فتحت شبكة الإنترنت الباب على مصرعيه للإعلانات التجارية، وعرض البضائع بالصوت والصورة.
- **إجراء المكالمات الهاتفية الدولية والمحلية:** نسبة للتطور التكنولوجي أصبح من اليسير استعمال شبكة الإنترنت للاتصال الهاتفي مع نقل الصورة أيضاً، وذلك بربط الحاسوب بكاميرا وميكروفون لنقل الصوت والصورة بتكلفة زهيدة دون المرور عبر شبكة الاتصالات المخصصة لذلك، مع الملاحظة أن هذه العملية لها أثر سلبي على دخل مؤسسات وشركات الاتصال الوطنية، وهو ما تعتبره بعض الدول المحتكرة لخدمة الاتصال إضراراً بمصالحها وتحاول دون جدوى الحد منه.

---

(١) د/ أسامة مجاهد – مرجع سابق – ص ١٣٢ وما بعدها..

- **المجاميع الإخبارية News Grups:** تقوم هذه المجاميع بتغطية موضوعات مختلفة فى مجال العلوم والتكنولوجيا والسياسة وغيرها من المواضيع، وذلك وفقاً لاهتمامات المستخدمين والمشتركين فى هذه الخدمة.
- **الدراسة والتعلم عن بعد:** لقد سهلت شبكة الإنترنت الربط بين الطالب والجامعات المفتوحة ويسرت عملية التعليم. فبإمكان الطالب متابعة المحاضرات وهو فى بيته. أو يتابع بحوثه العلمية بالتراسل مع الدكتور المشرف على رسالته عبر الإنترنت. وقد ساهمت بنوك المعلومات المتخصصة المنتشرة على شبكة الإنترنت فى تقدم البحث العلمى، بما توفره للطالب من معلومات واحصائيات دقيقة عن أى دولة وفى أى موضوع يريد معلومات عنها.
- **استخدام الإنترنت في المجال الطبي:** بفضل إدخال الكاميرات والمكيروفون كوسائط طرفية للحاسوب، أصبح من اليسير أن يتابع مجموعة من الأطباء فى أماكن مختلفة من العالم العمليات الجراحية الدقيقة وإعطاء رأيهم فى ذلك عبر الإنترنت.
- **استخدام الإنترنت في تنفيذ أفعال يجرمها القانون (من الجوانب السلبية):**

إلى جانب المزايا والفوائد المكتسبة باستخدام الإنترنت نجد هذا النوع من النشاط البشرى لا يخلو مثل غيره من الأنشطة من سوء الاستخدام، حيث انتشرت أنواع جديدة من الجرائم لم تكن معروفة من قبل، مثل جرائم النصب والاحتيال والسرقة المعلوماتية والدعارة والتعدى على الآداب العامة ونشر الرذيلة والجاسوسية... الخ، وتتسم هذه الجرائم بسرعة التطور مما أدخل رجال القانون فى صراع عنيف ومتواصل، لكى يواكبوا التطور التكنولوجى الهائل وذلك التطور السريع فى ثورة المعلومات الحديثة.

**البند الخامس: أشهر أنواع الجرائم التي ترتكب بواسطة الإنترنت(١):**

- **اختراق مواقع علي شبكة الإنترنت وتغيير صفحتها الرئيسية:**

ويقوم بهذا العمل الهاكرز الذين لا يريدون سوى إثبات قدرتهم على الاختراقات ويتم تحديد هوية هؤلاء المخترقون من خلال ملفات Log Files على الحاسبات الرئيسية التى ترصد كل دخول وخروج على ملفات النظام.

- **اختراق مواقع علي شبكة الإنترنت وسرقة محتويات الملفات أو تغيير بيانات بها:**

ويقوم بهذا العمل الكراكرز الذين يقومون بتدمير المواقع وتغيير بياناتها ويتم تحديد هوية هؤلاء المخترقون من خلال ملفات Log Files على الحاسبات الرئيسية وأنه كانوا فى معظم الحالات يستخدمون أسلوب الخداع والتمويه لتضليل أى جهة تحاول رصدهم وهناك أساليب وبرامج كثيرة تكشف هذه الاختراقات وتحدد هويتهم.

- **اختراق أجهزة حاسبات فردية من خلال برامج التجسس:**

ويقوم بهذا العمل الهاكرز الذين لديهم حب الاستطلاع ومعرفة محتويات أجهزة الغير وذلك عن طريق إرسال برامج تجسس من أنواع الأبواب الخلفية من خلال برامج المحادثة أو إرسال رسالة بريد إلكترونى تحتوى على برنامج تجسس لينقل كل محتويات الجهاز إليه.

ويتم تحديد ما إذا كان الجهاز قد تم اختراقه من عدمه عن طريق فحص ملفات الرجيسترى وملفات النظام بحيث يتم رصد أى تغيير تم بها ومنها يتم تحديد نوع الفيروس أو الباك دورز الذى تم تثبيته على الجهاز.

- **سرقة عناوين البريد الإلكتروني:**

ويقوم بهذا العمل الأشخاص الذين لديهم ميول إجرامية حيث يتم سرقة

---

(١) حسن مدحت الروبى وآخرون – مرجع سابق – ص ٢٧ وما بعدها.

البريد الإلكتروني لشخص ما،ويقوم بإرسال رسالة بريدية منه على عنوان شخص آخر،في محاولة لإثبات أن تلك الرسالة مرسلة من صديق وقد تكون هذه الرسالة محملة بفيروس أو ملف تجسس لينقل كل المعلومات التي على الجهاز.

ويتم تحديد مرتكب هذا العمل بأساليب وبرامج فنية كثيرة تقوم بتحديد مرسل الرسالة الفعلي وبشكل دقيق.

- **سرقة أرقام الدخول على المحادثات الفورية:**

ويقوم بهذا العمل الأشخاص الذين يريدون أن يشهروا بأشخاص آخرين على شبكة الإنترنت من خلال برامج المحادثة الفورية (الدردشة) بإعطاء معلومات عنهم لكل من يتصل بتلك البرامج أو أنهم يقوموا بإنشاء أرقام خاصة بأسماء من يريدوا التشهير بهم مع كتابة بيانات غير صحيحة عنهم.

ويتم تحديد هوية هؤلاء الأشخاص بأساليب وبرامج فنية تقوم بتحديد الشخص مرتكب هذا العمل وتحديد مكانه الفعلي.

- **هجمات حجب خدمة الإنترنت:**

وهي عبارة عن توجيه شخص ما أو جهة ما مجموعة من حزم بيانات شبكية بصورة كثيفة جداً إلى أحد الأشخاص أو أحد مواقع الإنترنت باستخدام الرقم التعريفي وتعتمد تلك الهجمات على توجيه طلبات كثيفة باستخدام بروتوكول رسائل التحكم بالإنترنت أو ما يطلق عليه (Internet Control Message Protocol "ICMP") وهذا البروتوكول يسمح بتبادل رسائل التحكم والتعامل مع رسائل الخطأ كما تحدث هذه الهجمات باستخدام منافذ بروتوكولات TCT, UDP.

ويتم تحديد هوية هؤلاء المخربون من خلال برامج وأساليب فنية تظهر المخترق وتحدده بشكل دقيق وبصورة كاملة.

• **سرقات أرقام بطاقات الإئتمان:**

ويقوم بهذا العمل بعض الأشخاص الذين يقومون بعمل عدة معادلات رياضية لتوليد أرقام بطاقات ائتمانية لإجراء عملية الشراء على الإنترنت وتكون هذه البطاقات بالطبع مملوكة لغيرهم من الأشخاص.

ويتم تحديد هؤلاء الأشخاص باستخدام تقنيات حديثة،وإن كانت بعض الشركات الموجودة على الإنترنت والتى تتعامل فى أنظمة البيع على الشبكة قد تنبهت إلى خطورة سرقة أرقام بطاقات الإئتمان،حيث قامت بتأمين جميع المراسلات التى تستخدم أرقام البطاقات الائتمانية.

## الفرع الثالث

## البرمجيات

أدت الطفرة المذهلة التى حدثت فى تكنولوجيا البرمجيات إلى تطور سريع فى تكنولوجيا المعلومات من مرونة وسرعة ودقة فبعد سلسلة من التجارب الفاشلة فى تطوير البرمجيات على اختلاف مجالاتها ودرجة تعقدها، ومع تعاظم دور البرمجيات فى منظومة المعلوماتية، تأكد أن عملية تطورها أعقد من أن تترك لمحاولات الهواة من مخططى البرامج ومحللى النظم، فخرجت إلى الوجود شركات متخصصة فى إنتاجها(*).

**البند الأول: أقسام البرمجيات:**

وتستخدم البرمجيات فى تشغيل الحاسبات، وهى عبارة عن مجموعتين كل منهما تأخذ طابعاً مميزاً، وهما: برامج التشغيل التى ترتبط ارتباطاً وثيقاً بمكونات أجهزة الحاسب الصماء، وبرامج التطبيق التى بدورها تتضمن البرمجة ذات المستوى الأدنى مثل أجهزة التحكم، والأنظمة المدمجة، والبرمجة ذات المستوى الأعلى مثل النظم الإدارية والتصميمية والمحاسبية.

وتحتاج صناعة البرمجيات بطبيعتها إلى كوادر بشرية مؤهلة تأهيلا تقنياً فى هذا المجال، وقد مرت تكنولوجيا البرمجيات بتجارب عالمية، وقطعت شوطاً طويلاً فى تصنيع البرمجيات وتطويرها، حتى أصبحت هذه الصناعة مستقرة،

---

(*) كان كل من «بيل جيتس Bill Gattes» و «بول الن Pouli Alen» وهما طالبان فى جامعة هارفارد قد بدءا نشاطهما عام ١٩٧٥، حيث قاما بتطوير لغة البرمجة «بيسيك Basic» كى تعمل على جهاز الحاسب الآلى الصغير "Home Comp" وأطلقا اسم مايكروسوفت "Micro Soft" على شركتهما الوليدة، ودخلت العديد من الشركات الأخرى ذات المجال خلال تلك الفترة، لتساهم كل منها بنصيب فيما آلت إليه ثورة المعلومات .

تؤدى دورها الإيجابى فى دعم الدخل القومى، وتوجد عدة نماذج عالمية فى صناعة البرمجيات – منها التجربة الهندية واليابانية والأوروبية[1].

أما فى مصر، فقد بدأت تجربة إعداد البرامج بلغات الحاسب المختلفة خلال الستينات، عندما كانت الحاسبات ذات أحجام كبيرة وقدرات محدودة، وقد ارتبط تخطيط البرامج بشركات إنتاج الحاسبات.

ومع ظهور الحاسبات الشخصية وانتشارها فى مصر، وتطور الأساليب الحديثة للبرمجة. إنشئت عدة معاهد لتدريب الخريجين المتميزين على تكنولوجيا البرمجيات وتطوير المنظومات. وقد بدأ سوق البرمجيات فى مصر يشق طريقه بصعوبة بالغة، نظراً لصغر حجم الشركات المنتجة ومحدودية إمكاناتها.

وكان من الطبيعى أن تتعرض تلك البرامج للاعتداء من الآخرين، فانتشرت جرائم تقليد البرامج أو نسخها أو تعديلها، الأمر الذى رتب أضرار مالية ومعنوية بمنتجيها، لذا كان من الضرورى أن تمس التشريعات التى تحمى حقوق منتجى تلك البرامج وتوقيع العقاب المناسب على مرتكبى هذا النوع من الجرائم.

ونظراً لأن المكونات غير المادية للحاسب الآلى أو كيانه المنطقى – وعلى رأسها برامجه وبياناته – تعتبر نتاج فكر وجهد ذهنى وبدنى للإنسان، لذا فإنه من الأهمية حمايتها، بذات القدر الذى تكفله النصوص التشريعية الخاصة بحماية براءات الاختراع وكذا نصوص حماية حق المؤلف.

وقد ظهرت الحاجة إلى مواكبة التكنولوجيا الجديدة، بمعالجة قانونية لتنظيمها وإضفاء الثقة والحماية على استخدامها محلياً، وذلك من خلال

---

(١) جمال عبد المنعم محمد وآخرون – جرائم المعلوماتية (بين الواقع وتحديات المستقبل) – بحث مقدم فى الدورة ٨٩ – فرقة القيادات الأمنية – معهد القادة – أكاديمية الشرطة – القاهرة – سنة ٢٠٠٢ – ص ٤١.

النصوص القانونية المطبقة، أو باستخدام المبادئ القانونية العامة(*)، أو باستخدام القياس أو باستحداث نصوص قانونية جديدة، تواكب ذلك التطور السريع المتلاحق.

وقد ظهرت إلى حيز الوجود اتفاقيات دولية في هذه المجالات منها اتفاقية المنظمة العالمية للملكية الفكرية فى حق المؤلف "WIPO - WCT" واتفاقية المنظمة العالمية للملكية الفكرية فى مجالات التمثيل والأداء والتسجيلات الصوتية "WIPO - WPPHT" ثم اتفاقية بودابست لمقاومة جرائم نظم وشبكات الحاسب المعلوماتية والاتصالات فى نوفمبر ٢٠٠١.

**البند الثاني: قرصنة البرمجيات عبر شبكة الإنترنت(١):**

أدى ارتفاع أعداد مستخدمى شبكة الإنترنت بمعدلات عالية وازدياد المعدل القياسى لسرعة نقل البيانات، وانخفاض تكلفة الاتصال بالشبكة فى معظم مناطق العالم، بل ومجانيته فى مناطق أخرى إلى تسهيل وتوسيع عمليات تبادل البرامج المقرصنة عبر الشبكة.

وتنتشر الآن فى شبكة الإنترنت عشرات المواقع التى تتضمن مختلف الأنواع من البرامج كالألعاب ونظم التشغيل والبرامج الخدمية، ويمكن الحصول على أى من تلك البرامج مجاناً، أو مقابل مبالغ زهيده عن طريق بطاقة ائتمانية فقط مع نقر الماوس (الفأرة).

وتتسبب القرصنة فى الدول المنتجة للمعلوماتية فى خسارة أعداد كبيرة من العمال وظائفهم، وخسارة الحكومات مليارات الدولارات من أموال الضرائب

---

(*) وقد نصت المادة الثانية من القانون رقم ٣٥٤ لسنة ١٩٥٤ الخاص بحماية حق المؤلف والمعدل بالقوانين رقمى ٣٨ لسنة ١٩٩٢، ٢٩ لسنة ١٩٩٤ على أن تشمل الحماية المنصوص عليها فى هذا القانون مؤلفى مصنفات الحاسب الآلى من برامج وبيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة.

(١) جمال عبد المنعم محمد وآخرون – المرجع السابق – ص ٤٤ وما بعدها.

وتقدر الإحصاءات فى الولايات المتحدة الأمريكية مثلاً أن ١٣٠٠٠٠ شخص يفقدون وظائفهم سنوياً، كنتيجة مباشرة لعمليات القرصنة، كما تحرم الخزانة الأمريكية من تحصيل ضرائب تصل إلى مليار دولار سنوياً لذات السبب، وتتسبب القرصنة عبر شبكة الإنترنت فى معظم تلك الخسائر والتى تنمو باستمرار مع نمو تلك الشبكة(١).

ويرى الكثير من أصحاب مواقع القرصنة، أنهم يفعلون ذلك نشراً للمعلوماتية التى تحتكرها شركات البرمجيات الكبرى النهمة، والتى تطالب بمبالغ باهظة مقابلها. متناسين أن وراء هذه البرمجيات مئات من ساعات العمل وعشرات من المبرمجين.

ويتسابق كثيراً من القرصنة فى نشر البرامج المقرصنة مجاناً، للتباهى فقط بقدراتهم فى سرعة كسر نظام حماية النسخ الذى يوضع عادة على البرامج، بحجة أن البرامج الأصلية مرتفعة الثمن، ولا يستطيع معظم مستخدمى الكومبيوتر تحمل تكاليفها، وأكثرهم من طلاب المدارس والجامعات.

ويبرر كثير من رواد تلك المواقع مسلكهم، بأنهم يتبعون فلسفة الاستخدام العادل، إذ أن شروط الاستخدام التى تمليها شركات البرمجيات لا تتمتع بالعدل والإنصاف.

وتُعرض معظم دول العالم النامى عن سن القوانين المضادة لقرصنة البرمجيات، باعتبارها من الدول المستهلكة للبرمجيات، حيث يسود الاعتقاد بأن سن مثل هذه القوانين يصب فى مصلحة الدول المنتجة للبرمجيات، فالصين تعرض عن سن هذه القوانين بعد أن تبين للمسئولين فيها أن مثل تلك القوانين تصب بشكل مباشر فى مصلحة الولايات المتحدة، بل ذهبت الأرجنتين إلى ما

---

(١) راجع موقع اتحاد صناعة التسجيلات الأمريكى على شبكة الإنترنت RIAA على العنوان: .http:// www. riaa.com

هو أبعد من ذلك، حيث أصدرت إحدى المحاكم العليا الأرجنتينية قانوناً يبيح قرصنة البرامج ويعلن شرعيتها[١].

وقد شرعت بعض شركات البرمجيات ومواقع الإنترنت باتخاذ إجراءات هجومية، ضد من يستخدم برامجها المقرصنة، ومن أهم هذه الشركات مايكروسوفت وياهوو - اللتان هددتا بفحص القرص الصلب لزوار مواقع الإنترنت دون علمهم، وذلك بإضافة نصوص برمجيه إلى مواقعها، تفحص القرص الصلب لواحد من كل مائة زائر لهذه المواقع، بحثاً عن وجود برامج مقرصنة، إلا أن منظمات حماية الخصوصية - عبر شبكة الويب - قد وقفت ضد هذه الإجراءات، التى تتضمن انتهاكاً كبيراً لخصوصية مستخدم الإنترنت، مما أدى إلى تراجع الشركات عن اتخاذ هذا الإجراء.

---

(١) راجع فى هذا الشأن تقرير اتحاد صناعة البرمجيات والمعلومات SIIA ضمن موقع الاتحاد على شبكة الإنترنت على العنوان: http:// www. siia. net.

# الباب الأول

# الحماية الموضوعية للمعلوماتية

- تمهيد.
- الفصل الأول: ماهية الجريمة المعلوماتية.
- الفصل الثاني: جرائم المعلوماتية في القانون.

* الفصل الثالث: جرائم المعلوماتية في ضوء الاتفاقيات الدولية.

**تمهيد وتقسيم:**

منذ الثورة الصناعية وما رافقها وتلاها من تنوع وازدياد مطرد فى حجم الأنشطة العلمية والتكنولوجية، وما نجم عنها فى القرن الماضى من تطورات اقتصادية واجتماعية وانعكاسات ثقافية وحضارية، بدأت المعلومات(*) المنتجة والمتداولة تتزايد بمتوالية هندسية واسعة القفزات، وطرأ على رصيدها الكلى طفرة لكمية فاقت طاقة الفكر الإنسانى على متابعتها أولا بأول(**)، والاستفادة منها

(*) المعلومات مورد لا يقل ولا ينضب Neither scarce nor deplating، تتزايد دوماً ولا تتناقص بالمستخدم أو تستهلك. ترتبط بالزمان والمكان وتتفاعل مع التطور، وعلى متلقيها ومدى حاجته تتوقف – إلى حد كبير – قيمتها.

- G. Edward Evans, Developing Library and Information Center Collections, Second edition, Libreries Unlimited, INC, 1987, p. 2.

والمعلومات فى الحقبة المعاصرة مفتاح للموارد الأخرى Key to other resources، وسلعة (خدمة) تباع وتشترى. ومصدر قوة اقتصادية وسياسية لمن يحسن جمعها وتنسيقها وإستخدامها. وهناك حكمة أنجلوسكسونية تقول أن «المعلومات قوة – In formation is Power»، ومثل فرنسى يعبر عن أن «الرجل الذى يعلم يعادل (يساوى) رجلين، Un Homme Informé en vaut deux. وما سبق يصاغ فى حكمة الأمم وتشيد حضارتها Sagesse des nations، تتشكل عبر العصور. وتشاهده الإنسانية واقعاً ملموساً فى الحقبة المعاصرة من خلال صناعة المعلومات Industrie de l'information، التى بزغت شمسها فى منتصف القرن قبل الماضى (التاسع عشر) مع ظهور الصحف ووسائل الإتصال عن بعد (التلغراف)، ثم تلى ذلك فى العقود الأخيرة المنصرمة تطورات تقنية بارزة. للمزيد يراجع:

- Eric de Grolier, L'organisation des systémes d'information de Pouvoins Publics, Unesco, 1978, p. 9.

(**) تُبين إحدى الدراسات.. فى معرض تدليلها على ضخامة حجم ظاهرة هذا الانفجار المعرفى (المعلوماتى) فى الحقبة المعاصرة، أن ما أنتجه العقل البشرى فى الخمسين سنة الأخيرة من معلومات يعادل ستة أمثال ما أنتجه فى خمسة قرون سابقة. وتشير إلى أن ما طبع من كتب منذ عرف الإنسان الطباعة حتى الآن يصل بصرف النظر عن عدد نسخ كل كتاب، إلى خمسة عشر مليون كتاب منها أثنى عشر مليوناً فى النصف قرن الأخير وحده، وأن عدد الكتب

-/-

بالدرجـة المرضية والمطلـوبة(١).

وإزاء هذه الطفرة(*) بدت الطرق التقليدية لجمع وتنظيم المعلومات، عاجزة عن تلبية احتياجات المستفيدين من المعلومات بكفاءة وفاعلية. وأصبح محتماً

---

— التى تصدر بعناوين جديدة كل سنة يصل إلى ٧٥,٠٠٠ عنوان، فضلاً عن قرابة ٥٠,٠٠٠ دورية تنشر سنوياً حوالى ٢٥٠ مليون مقال، (دكتور/ شعبان عبد العزيز خلفية – شبكات المعلومات (دراسة فى الحاجة والهدف والآداء) – مجلة المكتبات والمعلومات العربية – دار المريخ للنشر – س ٤ – عدد ٢ – ابريل ١٩٨٤ – ص ١٢ ، ١٣.

وأوضحت دراسة أخرى إلى أن تضاعف المعرفة المتاحة للإنسان منذ بداية القرن التاسع عشر تطلب مرور عدة عقود، بينما تضاعفت المعرفة المتاحة من منتصف القرن الـ ٢٠ فى عشر سنوات فقط. ولم تتطلب مضاعفة المعرفة المتاحة في عام ١٩٧٠ إلا خمس سنوات فقط. يراجع:

- Zmud Robert W., Information Systems in organization, Glenview, Illinois: Scott, Foresman co., 1983. p. 5.

وتعبيراً عن ذات ا لمشكلة يقول مارشال ماكلوهان أن: «المعلومات تنصب علينا بشكل فورى ومستمر. ففى اللحظة التى يستوعب فيها الفرد معلومة ما تكون هناك معلومات أخرى قد حلت مكانها». عن:

- Stephen W. Littejohn, Theories of Human communication, Second Edition, Bolmont, California: Wadsworth Publishing Company, 1983, p. 267.

مشار إليه لدى: د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات) – مرجع سابق – هامش (١) ص ٤.

(١) المرجع السابق – ص ٣.

(*) توصف الطفرة المعاصرة في نمو وتكاثر المعلومات عادة بعبارة «أنفجار المعلومات» Information Explosion أو «الانفجار الوثائقى» Explosion documentaire.

ويذهب د/ هشام رستم لأن كلاهما لا يبدو دقيقاً، لأن الإنفجار ظاهرة تتضخم فيها الأشياء بشكل مفاجئ ثم ينتهى أمرها وإن ظلت لها بعض الآثار، أما ما يواجهه المجتمع الإنسانى فى الحقبة المعاصرة، فهو زيادة مستمرة فى حجم المعلومات لا نهاية لها. (المرجع السابق – هامش (٢) ص ٤). وثمة اعتراضات موضوعية أخرى على التعبير الأول يراجع فى تفصيلها: (ك ف. أ، فينو جرادوف وآخرون – نحو نظام معلومات دولى – ترجمة إبراهيم البرلسى – المجلة الدولية للعلوم الاجتماعية – مركز مطبوعات اليونسكو – القاهرة – س ١٢ – فبراير / مارس ١٩٨٢ – ص ١٤.

استخدام أساليب علمية وتقنية متطورة، لمواجهة فيض المعلومات المتدفق والتعامل معه. وعلى مدى النصف قرن الماضى اتخذ السعى لإيجاد حلول مناسبة للتغلب على مشكلة تزايد حجم المعلومات مسارين رئيسيين(١): –

الأول: تمثل فى تركيز العديد من دراسات (علم المعلومات) على التحسين والتطوير فى عملية فهم طبيعة المعلومات، ومكوناتها، وكيفية حصرها وتجميعها وتبويبها وتصنيفها وتحليلها، بهدف الاستفادة منها بفاعلية عظمى.

الثاني: تبدى فى ظهور ورواج مستحدثات تقنية متقدمة للتحكم فى المعلومات وتجميعها، ومعالجتها واختزانها واسترجاعها وتحسين الإنتفاع بها، كالحاسبات وتقنيات المصغرات الفيلمية والأقراص الليزرية ووسائل الإتصال والائتمار من بعد، التى يشكل تزاوجها واندماجها معاً، ما يعرف بتكنولوجيا (تقنية) المعلومات أو المعلوماتية(٢).

وكما نتج عن تحكم البشرية فى القدرة الميكانيكية وإحلالها بدرجة كبيرة مكان القوة العضلية للإنسان والحيوان – ما أطلق عليها الثورة الصناعية – كذلك يقف التحكم فى المعلومات من خلال التطوير المتواصل للمعلوماتية، كمساعد للقدرات التنظيمية للعقل البشرى وراء ثورة كلية شاملة تجتاح العالم منذ نهاية القرن الماضى ومستمرة بأطراء، هى الثورة المعلوماتية La revolution informatique، الموسومة أيضاً بالثورة الصناعية الثالثة، التى تعزز الإمكانات الفكرية والقدرة المنطقية Lapuissance Logique للإنسان، وتنقل الحضارة

---

(١) د/ هشام رستم – المرجع السابق – ص ٥.

(٢) المرجع نفسه – ص ٦. مشيراً إلى:

- André Vitalis; Informatique, Pouvoir et libertés, Paris, Economica, 1981, p. 22.

الإنسانية من عصر الصناعة إلى عصر (أو مجتمع) المعلومات(*).

ومع دخول الألفية الثالثة لم يعد ثمة مجال اقتصادى أو اجتماعى أو صناعى أو إدارى إلا وتباشر أجهزة الحاسوب وتقنية المعلوماتية دوراً رئيسياً فى أدائه وإنتاجه وتطويره أيضاً. وصار التفاعل مع قواعد البيانات والتعامل مع النظم المتقدمة ووسائل الذكاء الاصطناعى حقيقة واقعية(**).

وفى هذه البيئة المعلوماتية الضخمة المزدحمة - بالشبكات والحاسبات والتقنيات - تضعف قبضة الأمن والمراقبة والتحكم (ويمكن القول بأنه تعجز)،

---

(*) يجمع أكثر الكتاب والمحللون الاجتماعيون - على اختلاف خلفياتهم ومذاهبهم - على أننا نشهد الآن - ومنذ فترة ليست بالقصيرة - تحولاً جذرياً فى المجتمع، ويحددون أساس هذا التحول فى النظم الآلية لمعالجة وتخزين وبث المعلومات، ويرى هؤلاء - ونؤيدهم فى ذلك - أن الإنسانية مقبلة على حضارة تتأسس على المعرفة، تؤدى فيها المعلوماتية دوراً هاماً - وصفوه بأنه دور المادة الخام الأولية - ويتعاظم فيها دور المعلومات كمورد استراتيجى، أكثر أهمية من مصادر الطاقة والمعادن ورأس المال. ونظراً لاختلاف منظورهم لطبيعة هذا التحول تعددت المسميات التى أطلقوها على هذا العصر الذى استشرفوه. حيث وصفه روبرت ثوبالد بعصر الاتصال Comminication Era. راجع:

- Robert Theobald, Problem / Possibility focusers: A new Knowledge for the communication Era, in Howard F. didsbury, ed. communication and Future society, 1982, pp. 276 et seq.

بينما أطلق عالم الاجتماعى الأمريكى دانييل بل Daniel Bell على هذا العصر إسم عصر أو مجتمع ما بعد الصناعى Post - Industrial Society، وقرر أن المبدأ المحورى فيه هو الوضع المركزى للمعرفة، باعتبارها مصدر كلا من: قوة الابتكار والتجديد التطويرية، وتشكيل السياسات وضع القرارات للمجتمع. (حول آراء ومصطلح دانييل بل - أنظر):

- A. I. Mickhailov, New Technology and the Future of Scientific Information, in "The challenge of Information Thechnology", K. R. Brown (Editor), North-Holland Company, 1983, p. 87.

(مشار إليه لدى: د/ هشام رستم - المرجع السابق - هامش ٢ - ص ٦).

(**) غدا العالم أشبه بمجتمع كبير تترابط فيه الحاسبات وشبكات الأتصال باختلاف أشكالها وأنواعها، وتتدفق بين أرجائه المعلومات بتقنياتها المتنوعة، حيث تلاشت الحواجز الجغرافية، وتقاربت المسافات، فأصبح العالم قرية صغيرة تجرى بين جنباتها انحاء المعمورة.

وتزدهر أوجه الاعتداء على نظم المعلوماتية المعالجة اليكترونياً، حتى أضحت تشكل تهديداً بالغاً وخطراً محدقاً لسائر الهيئات الحكومية وغير الحكومية المعتمدة فى انجاز مهامها على أجهزة الحاسبات وشبكات الأتصال. وترتفع مخاطر إساءة استخدام الحاسبات والتلاعب فى البرامج وملفات المعلومات المخزنة آلياً بقصد الحصول على منفعة غير مشروعة من أموال أو أصول مستندية أو خدمات غير مستحقة. وهيئة عمليات التقليد والنسخ من غير طريق المنتج الأصلى المناخ المناسب والمجال الفسيح لبث الفيروسات المعلوماتية، التى تصيب الأنظمة والشبكات بدرجات متفاوته من العطل والضرر.

وهكذا، جاء تقدم تقنيات الحاسبات والمعلومات وتزايد الاعتماد عليها فى تسيير شئون المجتمعات(*)، مصحوباً بفرص جديدة لإرتكاب أشكال وصور مستحدثة من الجرائم الفنية Technocrimes، تحمل طابع هذه التقنيات وتساير على الدوام تيار تقدمها باعتمادها على الحاسب (كأداة) لارتكابها، وقيام فكرتها على الوصول غير المشروع إلى المعلومات المعالجة اليكترونياً وإساءة استخدامها[1].

وقد زاد حجم الجرائم المعلوماتية وتنوعت أساليبها وتعددت اتجاهاتها وتعاظمت خسائرها وأخطارها، حتى صارت من مصادر التهديد المباشرة للأمن القومى للدول. وبخاصة تلك التى ترتكز مصالحها الحيوية على أنظمة المعلوماتية، وتعتمد عليها فى تسيير شئونها. وأمام هذا الشكل الجديد للجريمة وما

(*) من المؤشرات الدالة على تعاظم الاعتماد على تقنية المعلومات فى العصر الحاضر، ما أظهرته دراسة حديثة أجريت بالدول الاسكندنافية، على مجموعة من الشركات بها، من أن ٢٣ ٪ من هذه الشركات لا يمكنها العمل بدون نظم المعالجة الآلية للبيانات لفترة قصيرة (من يوم إلى يومين)، و ٤١ ٪ منها يمكنها العمل بدون هذه النظم لمدة لا تتعدى يوم إلى أربعة أيام.

- T. Daler, Rgulbrandsen, B. Melgard and T. Sjqlstd, Security of information and Data, John wiley & Sons, 1989, p. 14.

(١) دكتور/ هشام رستم – المرجع السابق – ص ٩.

ينبئ عنه المستقبل من بزوغ سلوك إجرامى تقنى متطور يصيب المعلوماتية وعناصرها ومستخدميها (حكومات ومنظمات وأفراد)، يكون للتشريع دوراً هاماً ومؤثراً فى الردع بشقيه العام والخاص. وإن كان واقع الأمر يشير إلى أن جرائم المعلوماتية تدخل فى نطاق اختصاص القسم الخاص لقانون العقوبات Le droit pénel spécial، ذلك الفرع الذى يدرس كل جريمة على حده بعناصرها الأساسية والعقوبة المقررة لها(١).

وأمام هذا الشكل المستحدث للجريمة، لا يبدو قانون العقوبات – فى حالته الراهنة – كافياً أو فعالاً بالدرجة المطلوبة والمرضية. فنصوصه والنظريات والمبادئ القانونية التى يتضمنها أو تقف ورائه، مورث بعضها من القرن قبل الماضى (التاسع عشر)، حيث لم يكن ثمة متخصصين وقتذاك وإنما أصحاب مهن وحرف تقليدية. وتطبيق بعض هذه النصوص – أو النظريات والمبادئ القانونية – على الأشكال الجديدة للجرائم التى تستعير من تقنيات الحاسبات والمعلومات أساليب ارتكابها، لا يصطدم – فحسب – بصعوبات ناجمة عن الطبيعة الخاصة والخصائص التقنية الفريدة للوسائل المعلوماتية المستخدمة فى ارتكابها(*)، والتى تتبدى فيما نشهده مع المعلوماتية – وفقاً لقول جانب من

---

(١) أستاذنا الدكتور/ أحمد فتحى سرور – الوسيط فى قانون العقوبات – القسم الخاص – دار النهضة العربية – القاهرة – سنة ١٩٩١ – ص ٥ وما بعدها.

- حيث أن أهم ما يشغل المشرع عند وضع قانون العقوبات هو تحديد الجرائم أى الأفعال التى ينهى المشرع عن ارتكابها وما يقابلها من عقوبات، كما وأن الجريمة تنشئ للدولة حقاً فى عقاب الجانى، ويتولى قانون العقوبات تحديد مضمون هذا الحق، يراجع أيضاً:

- Franz Pilklin - La protéction des données personelles. Aspects de droit pénal. Situation. Actuelle en suisse, Rev. Inter de dro. comparé, 1987, No. 3, p. 665,

(*) الأنشطة الإجرامية فى القطاع المعلوماتى، وإن اختلفت طبيعتها وتنوعت – كما يقول البعض – إلا أن ثمة قاسماً مشتركاً بينها يتمثل فى الأساليب التقنية الجديدة المستخدمة فى ارتكابها، والتى تجعل تطبيق المفاهيم القانونية التقليدية عليها صعباً، إن لم يكن مستحيلاً.

-/-

الفقه – من تفريغ وسلب لمادية Dématérialisation السلوك[1]، وإنما تعترضه كذلك صعوبات رئيسية أخرى مردها أن نصوص التجريم التقليدية قد وضعت فى ظل تفكير يقتصر إدراكه على الثروة الملموسة والمستندات ذات الطبيعة المادية، مما يتعذر معه تطبيقها لحماية القيم غير المادية المتولدة عن المعلوماتية[2].

وإن كانت بعض التشريعات تسعى إلى إيجاد قانون مستقل خاص بالمعلوماتية Le droit dinformatique، وهذا نتيجة طبيعة للتطور فى هذا المجال[3]. حيث تكفل الفقة الجنائى فى بلدان عدة[*]، بإبراز الصعوبات التى

- B. Bergmans, Le Vol d'information en droit comparé, R.D.P.C., 1988, No 8-9-10, p. 905.

(1) Pradel, Conclusion du colloque Informatiique et droit pénal, Paris, cujas, 1983, p. 155.

(٢) د/ هشام رستم – المرجع السابق – ص ١٢.

(٣) د/ هدى حامد قشقوش – جرائم الحاسب الآلى فى التشريع المقارن – دار النهضة العربية – القاهرة – سنة ١٩٩٢ – ص ٦.

(*) كفرنسا وإيطاليا وألمانيا – والولايات المتحدة الأمريكية وأستراليا. وتضم القائمة التى وضعها البعض لما تقتضى مصلحة المجتمع الملحة إدخاله فى دائرة التجريم والعقاب فى هذا المجال، ما يلى:

أ – الاستخدام أو الدخول إلى نظام ومصادر الحاسب على نحو غير مأذون به، ويشمل ذلك الحاسب والمعلومات المخزنه داخله.

ب– الإفشاء غير المصرح به للمعلومات بواسطة الحاسب.

جـ– النسخ أو الاستخدام غير المصرح به للبرامج.

د – التغيير أو التحرير غير المشروع لمصادر الحاسب، أو التلاعب فيه أو فيما يحويه من معلومات وبرامج.

هـ– اتلاف أو تخريب مصادر الحاسب، ويشمل ذلك إتلاف الحاسب أو ما يحويه من بيانات وبرامج.

و – الإعاقة غير المشروعة للوصول إلى مصادر الحاسب، كمنع أو تعطيل استخدام الحاسب أو برامجه أو البيانات المختزنة داخله.

- Joseph E. Collins, States improve computer crime law with private sector input, Data Management, Juin 1987, p. 5.

-/-

تعترض تطبيق النصوص التجريمية بالتشريعات التقليدية القائمة على أشكال الإجرام الجديدة التى أفرزتها المعلوماتية، وسعى إلى بلورة مجموعة من الضمانات القانونية التى تكفل تحقيق التوازن بين الضرورة الملحة – فى عصرنا الحديث – للإستفادة من إمكانات الحاسبات وتقنيات المعلومات، وبين الحاجة الفردية والاجتماعية إلى حماية حرمة البيانات الشخصية والخصوصيات. وبادر إلى توجيه الأنظار إلى طائفة من الأفعال فى بيئة المعالجة الآلية للبيانات، تقتضى مصلحة المجتمع الملحة إدخالها فى دائرة التجريم والعقاب(١).

وسوف نتناول بالدراسة الحماية الموضوعية للمعلوماتية، من خلال الفصول التالية:

**الفصل الأول - ماهية الجريمة المعلوماتية.**

**الفصل الثاني - الجريمة المعلوماتية في القانون.**

**الفصل الثالث - الجريمة المعلوماتية في الاتفاقيات الدولية.**

---

ــ ومن مجمل أعمال منظمة التعاون الاقتصادى والتنمية (O.C.D.E) حول الإجرام المعلومات، تولد الاتفاق على ضرورة أن يغطى قانون العقوبات فى كل دولة الافعال التالية:

أ – التلاعب فى البيانات المعالجة آلياً بما فى ذلك محوها.

ب– التجسس المعلومات L'espionnage informatique، ويندرج تحته الحصول أو الاقتناء / أو الاستعمال غير المشروع للمعطيات.

جـ– التخريب المعلوماتى Le sapotage informaque.

د – الاستخدام غير المشروع أو سرقة وقت الحاسب L'usagenon - autorisé ou Vol de temps ordinateur.

هـ– قرصنة البرامج Le piratage de programmes.

و – الدخول غير المشروع على البيانات أو على نقلها.

ز – اعتراض استخدام المعطيات أو نقلها.

(١) د/ هشام رستم – مرجع سابق – ص ١٤.

# الفصل الأول

## ماهية الجريمة المعلوماتية

- المبحث الأول: تعريف الجريمة المعلوماتية.

المطلب الأول: التعريفات التي تناولت الجريمة المعلوماتية.

المطلب الثاني: خصائص الجريمة المعلوماتية.

المطلب الثالث: سمات المجرم المعلوماتي.

- المبحث الثاني: الجريمة المعلوماتية والقواعد العامة في القانون.

المطلب الأول: الشروع في الجريمة المعلوماتية.

المطلب الثاني: الأشتراك في الجريمة المعلوماتية.

# الفصل الأول

# ماهية الجريمة المعلوماتية

من الأهمية عند دراسة الجريمة المعلوماتية، أن نبدأ بعرض تعريف لها يحدد أبعادها ويشمل مجالاتها، وحتى يتثنى ذلك فإنه سوف نعرض بداية فى تمهيد لتعريف الجريمة بصفة عامة، ثم تخصيص الوضع فى نطاق الجريمة المعلوماتية فى المبحث الأول، ويلى ذلك فى المبحث الثانى تطبيق القواعد العامة فى القانون على الجريمة المعلوماتية.

- **تعريف الجريمة بصفة عامة:**

اختلف الفقه الجنائى عند تناول الجريمة بالتعريف، وذلك تبعاً لاختلاف وجهات النظر إلى جوانبها من جانب إلى آخر.

فذهب جانب من الفقه إلى أن أعظم مراتب الخروج على نظام القانون وقواعده فى الضبط الاجتماعى إنما يتحقق بوقوع (الجريمة)، إذ الجريمة هى أكبر صور العصيان على النظام الذى يكفله القانون، كما أنها أبرز مظاهر الاقتئات على قواعد الانضباط فى المجتمع. وبذلك فإن الجريمة - فى أبسط وصف لها - هى خروج على النظام الذى يضعه القانون(١).

فيما ذهب رأى آخر إلى تناول الجريمة كحقيقة من خلال جانبها القانونى وجانبها الواقعى(٢):

فالجريمة كحقيقة قانونية هي فعل ما يعاقب عليه المجتمع ممثلاً فى مشرعه. لما ينطوى عليه هذا الفعل من المساس بشرط يعده المجتمع من الشروط الأساسية لكيانه، أو من الظروف المكملة لهذه الشروط.

---

(١) د/ جلال ثروت - الظاهرة الإجرامية (دراسة فى علم الإجرام والعقاب) - مؤسسة الثقافة الجامعية - الإسكندرية - سنة ١٩٨٣ - ص ٣.

(٢) د/ رمسيس بهنام - علم الإجرام - منشأة المعارف - الإسكندرية - سنة ١٩٨٨ - ص٢٨.

أما الجريمة كحقيقة واقعية فهى خروج ألفرد على ما يقتضيه وجود اشتراك بين الناس فى معيشة واحدة تصان فيها الأمة كفرد ومجموع أفراد(*).

فيما ذهب رأى آخر إلى أن تعريف الجريمة يجب أن يتضافر فيه الاتجاه الشكلى - ويسمى أيضاً القانونى - والاتجاه الموضوعى، وعلى ذلك يمكن تعريف الجريمة بأنها(١):

«واقعة إيجابية أو سلبية مصدرها خطأ انسان، يعدها المُشرع خطرة أو ضارة بالمصالح العامة أو العلاقات الاجتماعية، ويرتب عليها النظام القانونى عقوبة جنائية»(**).

وقد جاء ذلك مخالفاً لرأى فقهى ذهب إلى أنه على الرغم من تعدد التعريفات القانونية للجريمة، إلا أنه لا يوجد بينها اختلاف كبير، ولهذا يمكن تعريف الجريمة - وفقاً لمعناها القانونى - بأنها(٢):

«الفعل الذى يجرمه القانون ويقرر له جزاءاً جنائياً»، ويضيف ذات الرأى أما

---

(*) الجريمة من الوجهة الواقعية خروج وجماح وجنوح، يغلب به المرء الأثرة على الايثار، مضحياً فى سبيل كيانه الذاتى بما يتطلبه الكيان الاجتماعى - وقد يقال أن الأثرة غريزة فى كل إنسان لأن البشر مفطور على حب الذات، ولكن هذا القول لا ينفى أن الجريمة نوع من الاثرة شاذ بالنظر إلى ما يتوافر منها لدى الرجل العادى. فالمجرم المعلوماتى حينما يباشر السلوك الإجرامى فى نطاق المعلوماتية، أنما يباشر سلوك شاذ عن المجتمع.

(١) دكتور/ يسرى أنور على - شرح قانون العقوبات (أصول النظرية العامة) - دار النهضة العربية القاهرة - الجزء الأول - سنة ١٩٨٤ - ص ٢١٠.

(**) يشمل هذا التعريف ركنى الجريمة المادى والمعنوى، كما يعبر عن مضمونها، وهو يجيب عن دوافع المشرع إلى تجريم بعض الوقائع الإنسانية دون البعض الآخر، كما أن الاشارة إلى إرادة المشرع تفصح عن اختلاف التجريم مع اختلاف الزمان والمكان، بحيث يتعذر القول بوجود جريمة طبيعية ثابتة فى كل الأزمنة والمجتمعات.

(٢) د/ على عبد القادر القهوجى - علم الإجرام وعلم العقاب - الدار الجامعية - بيروت - سنة ١٩٩٠ - ص ١٢.

المعنى الاجتماعي للجريمة، فلقد تباينت آراء الفقهاء بشأنه.. فمنهم من يؤسسه على الاخلاق، ومنهم من يرده إلى القيم الاجتماعية(*).

لذلك فإن التعريف القانوني للجريمة أكثر انضباطاً لتحديد مفهومها، وأكثر وضوحاً في جعل أمرها بيد سلطة مهمتها حماية قيم المجتمع ومصالحه، عن طريق سن التشريعات اللازمة لهذا الغرض.

وفي حين تناول جانب من الفقة الجريمة بصفة عامة ومجردة، حيث عرفها بأنها: «فعل غير مشروع صادر عن إرادة جنائية يقرر لها القانون عقوبة أو تدبيراً احترازياً»[1]، أو بأنها: «عدوان على مصلحة يحميها القانون ويختص القانون الجنائي بالنص عليها وبيان أركانها والعقوبة المقررة لفاعلها»[2]، وبرز جانب آخر تناول تعريف الجريمة وفقاً لوجهة محددة من تلك الوجهات المتعددة لها، فمن الوجهة الاجتماعية تعرف الجريمة بأنها:

«كل سلوك جدير بالعقاب سواء عاقب الشارع الوضعي عليه أم لم يعاقب»[3]،

---

(*) ذهب الفقيه الايطالي (فيري) بشأن تعريف الجريمة إلى المعنى الاجتماعي – حيث أنه من أنصار المذهب الوضعي – فيؤكد أن المشرع يجرم الوقائع التي تخالف بقاء المجتمع ونظامه وأمنه، ومن أنصار هذا الرأي أيضاً الفقيه جريسبيني. يراجع في ذلك:
Ferri, Principi di diritto criminale, Torino, 1982, p. 197.

- وحديثا اقترح بعض الشراح – خاصة في ألمانيا – ما يسمى بالتعريف الشخصي للجريمة، وبمقتضاه تعد الجريمة أساساً أنتهاك لإلتزام قانوني. وهذا تعريف من جانب واحد أيضاً، إذ يقتصر على ابراز الجانب النفسي أو ارادة مخالفة القاعدة القانونية، ويهمل الجانب الموضوع.

(١) د/ محمود نجيب حسني – شرح قانون العقوبات (القسم العام) – دار النهضة العربية – سنة ١٩٨٨ – ص ٤٠.

(٢) د/ حسنين عبيد – الجريمة الدولية (دراسة تحليلية تطبيقية – دار النهضة العربية – سنة ١٩٩٠ – ص ٤٥.

(٣) د/ محمود نجيب حسني – المرجع السابق – (في استعراض المعاني المختلفة لتعبير الجريمة) – ص ٣٨.

ومن الوجـهـة القـانونيـة – الاتجاه الشكلى فى تعـريف الجـريمة – تعـرف بأنها: «خروج على أوامر قانون العقوبات أو نواهيه خروجاً يستتبع توقيع عقوبة ما على فاعله»(١) .

خلاصة القول أنه أيما كانت الوجهة التى تتناول تعريف الجريمة، وينظر من خلالها إلى المعنى المقصود، فإنها – الجريمة – فى نهاية الأمر تنم عن فعل خارج غير مشروع، يترتب عليه من النتائج والآثار أضراراً تلحق بمصلحة محمية. مع الوضع فى الاعتبار أن هذا الفعل يلزم لصيرورته غير مشروع أن يتم النص عليه فى القوانين الوضعية. حيث أن الحديث ينصب على الجريمة بصفة عامة – دون تحديد أو تخصيص – ويفهم من ذلك أنه يقصد بها الجريمة التى تقع فى نطاق الدولة (الجريمة الداخلية) .

**- المعني الشرعي للجريمة(٢):**

أصل كلمة جريمة(*) من جرم بمعنى.. كسب وقطع، ويظهر أن هذه الكلمة

---

(١) د/ رءوف عبيد – أصول علمى الإجرام والعقاب – دار الفكر العربى – القاهرة – ط ٥ – سنة ١٩٨١ – ص ٢٧ .

ويضيف: ولا ريب أن مفهوم الجريمة مفهوم متطور من زمن آلى آخر، ومن مجتمع إلى آخر. وبينما نجد أن الفقه يعنى بالجريمة بوصفها تتضمن خروجاً شكلياً على قاعدة آمره أو ناهيه، نجد أن علم الإجرام Criminologio – المعنى بدراسة الجريمة – يعنى بالجريمة بوصفها ظاهرة سلوكية تتضمن خروجاً شاذاً على أى وضع اجتماعى مستقر على نحو ما، بما يلحق ضرراً بهذا الوضع.

- ومن هذا المنطلق فإن دراسة الإجرام المعلوماتى، أنما يجد صداه فى ضوء دراسات علم الإجرام التى تتناول الخروج الشاذ على الوضع الاجتماعى المستقر ويلحق الضرر بهذا الوضع، والذى يمثل أنتفاع المجتمع بعناصر المعلوماتية المفيدة فى كافة مناحى الحياة. وتمتد فروع الدراسة وتتشعب للوصول إلى تجريم هذا الخروج وارساء تشريع عقابى لضبطه، ومعاقبة مرتكبه بعقوبة شرعية مناسبة.

(٢) الامام/ محمد أبو زهرة – الجريمة (الجريمة والعقوبة فى الفقه الإسلامى) – دار الفكر العربى – القاهرة – سنة ١٩٧٧ – ص ٢٣ وما بعدها.

(*) لابد من تحرير معنى الجريمة وأخواتها من التعبيرات العربية، من مثل الإثم والخطيئة والمعصية، وإن هذه التعبيرات تتلاقى فى معانيها الشرعية مع المعانى اللغوية التى استقر عليها =/=

خصصت من القديم للكسب المكروه غير المستحسن، ولذلك كانت كلمة جرم ويراد منها الحمل على فعل حمل آثما. ومن ذلك قوله تعالى: «وياقوم لا يجرمنكم شقاقى أن يصيبكم مثل ما أصاب قوم نوح أو قوم هود أو قوم صالح، وما قوم لوط منكم ببعيد».

أى لا يحملنكم حملاً آثماً شقاقى ومنازعتكم لى، على أن ينزل بكم عذاب شديد، مثل ما نزل بمن سبقوكم ممن شاقوا أنبيائهم.

ومثل قوله تعالى: «ولا يجرمنكم شنأن قوم على ألا تعدلوا، اعدلوا هو أقرب للتقوى». أى لا يحملنكم حملاً آثما بغضكم لقوم على ألا تعدلوا معهم..

ولذلك يصح أن نطلق كلمة الجريمة على ارتكاب كل ما هو مخالف للحق والعدل والطريق المستقيم.

ومن هذا البيان يتضح أن الجريمة فى معناها اللغوى تنتهى إلى أنها فعل الأمر الذى لا يستحسن ويستهجن، وأن المجرم هو الذى يقع فى أمر غير مستحسن مصراً عليه، مستمراً فيه، لا يحاول تركه، بل لا يرضى بتركه. وذلك ليتحقق معنى الوصف، إذ أن معنى الوصف يقتضى الاستمرار، وإذا كانت كل أوامر الشريعة فى ذاتها مستحسنة بمقتضى حكم الشارع، وبمقتضى اتفاقها مع العقل السليم، فعصيان الله تعالى يعد جريمة، وكذلك ارتكاب ما نهى الله تبارك وتعالى عنه يعد جريمة، وذلك لأنه غير مستحسن بمقتضى حكم الشارع بالنهى، وبمقتضى حكم العقل، لأن العقل السليم تتفق قضاياه مع قاضيا الشرع الحكيم(*).

--- العرف اللغوى. فلا يكاد الناس يختلفون فى أن معنى الجريمة الفعل الذى يستوجب عقاباً، ويوجب ملاماً.

(*) روى أن أعرابياً سئل لماذا آمنت بمحمد - ﷺ - فقال: لأنى ما رأيت محمداً يقول فى أمر أفعل، والعقل يقول لا تفعل، وما رأيت محمداً يقول لا تفعل، والعقل يقول افعل.

وعلى ذلك نستطيع أن نقول إن الجريمة فعل ما نهى الله عنه، وعصيان ما أمر الله به. أو بعبارة أعم عصيان ما أمر الله به بحكم الشرع الشريف(*).

ولكن لأن الفقهاء الذين ينظرون إلى المعاصى من ناحية سلطان القضاء عليها، وما قدره الشارع من عقوبات دنيوية – يخصصون اسم الجرائم بالمعاصى التى لها عقوبة ينفذها القضاء. فيقول الماوردى فى تعريفها:

"إنها محظورات شرعية زجر الله تعالى عنها بحد أو تعزير".

والحد هو العقوبات المقررة، ويدخل فى هذا القصاص والديات المنصوص عليها فى الكتاب الكريم أو السنة المطهرة، والتعزير هو العقوبات التى ترك لولى الأمر تقديرها بحسب ما يرى به دفع الفساد فى الأرض ومنع الشر. وسمى تعزيراً، لأن به تقوية الجماعة وبه حفظها، إذ أن عزر معناها قوى.

ونستطيع بذلك أن نقرر أن تعريف الجريمة على هذا النحو الشرعى، ينتهى إلى ما يقارب تعريف علماء القانون الوضعى لها، حيث ان الجريمة فى قانون العقوبات هى الفعل أو الترك الذى نص القانون على عقوبة مقرره له، فإنه بمقتضى ذلك لا يعتبر العمل جريمة – من الناحية القانونية – إلا إذا كان ثمة نص على العقاب، ولا عقاب من غير نص.

والتعريف الشرعى للجريمة السابق ذكره قد يفترق فى ظاهره عن تعريف القانون الوضعى فى التعزير، ولكن عند النظرة الفاحصة نجد التعريفين

---

(*) إن تعريف الجريمة على هذا النحو يكون مرادفاً لتعريف الفقهاء لها بأنها إتيان فعل محرم معاقب على فعله، أو ترك فعل محرم معاقب على تركه، وذلك لأن الله تعالى قرر عقاباً لكل من يخالف أوامره ونواهيه وهو:

- أما عقاباً دنيوياً ينفذه الحكام.
- وأما تكليفاً دينياً يكفر به عما ارتكبه فى جنب الله.
- وإما أن يكون عقاباً أخروياً، يتولى تنفيذه الحاكم الديان.

فكل جريمة لها فى الشرع جزاء إما عاجل فى الدنيا، وإما أجل فى الآخرة.

متلاقيين فى الجملة، وذلك لأن التعزيرات كلها تنتهى إلى منع الفساد ودفع الضرر، وكل ذلك له أصل فى الكتاب أو السنة. يقول تعالى: "ولا تعثوا فى الأرض مفسدين". ويقول – ﷺ –: لا ضرر وضرار.

ولأن هذه التعزيرات تُرك تقديرها لولى الأمر(*)، نستطيع القول بأن أكثر ما فى قانون العقوبات من نصوص عقابية رادعة مانعة للفساد من قبيل التعزيرات. ويضيف الأمام/ محمد أبو زهرة أنه ليس معنى ذلك أن هذا القانون شرعى من كل الوجوه، فإنه سكت عن جرائم قدر لها القرآن الكريم عقاباً شديداً، وعاقب على جرائم أخرى بعقوبات ليست هى المقدرة لها فى الكتاب والسنة(**).

## المبحث الأول

## تعريف الجريمة المعلوماتية

عند تخصيص القول بالنسبة للجريمة – بعموميتها – واستهداف الجريمة المعلوماتية بالدراسة والتطبيق، تستوقفنا أمور تدق ينبغى بحثها والنظر فى خصوصيتها، تعبر عنها تلك السمات التى تتفرد بها طائفة الجرائم المعلوماتية، هى مجموعة من العناصر المتداخلة المؤثرة فى طبيعة الأفعال الإجرامية المرتكبة والمتصلة أتصالاً وثيقاً بالحاسب الآلى والمعلوماتية، بحيث يصعب تصور وجودها دون ارتباطها بالحاسوب.

ويمكن أجمال العوامل المسببة لخصوصية الجرائم المعلوماتية فى[1]:

---

(*) السلطة التشريعة هى المختصة بسن القوانين فى نظام الدولة الحديثة، وهى الممثلة فى مجلس الشعب، ثم يتم عرض هذه القوانين على مجلس الشورى لإقرارها وأصباغ الشرعية القانونية عليها.

(**) وبذلك يتضح أنه ما أحوجنا إلى تدخل تشريعى قوى فى مجال مكافحة الإجرام المعلوماتى، يسن من العقوبات ما يراه رادعاً لمجابهة هذا المد الإجرامى المتنامى فى نظم المعلومات التى طغت فى حياتنا استعمالاً واستخداماً.

(١) د/ محمود محمد عبد النبوى – جرائم الحاسب الآلى – مجلة الأمن العام – العدد ٨٨. يناير ٢٠٠٥ – ص ١٠٨.

- عامل زمني: يتمثل في الحداثة النسبية لتلك الطائفة من الجرائم.
- عامل مكاني: يتمثل في تعدى آثار تلك الجرائم لتشمل أكثر من دولة واحدة.
- عامل نوعي: يتمثل في تنوع الأفعال الإجرامية المرتكبة، والتى من الممكن تصور ارتباطها بأجهزة الحاسبات الآلية.
- عامل تاثيري: يتمثل في اتساع أضرار جرائم الحاسوب لتشمل العديد من المجالات السياسية والاقتصادية والاجتماعية والعسكرية والعلمية... وغيرها.
- عامل تحليلي: يتم بالنظر إلى التحليل الكمي والكيفي لجرائم الحاسب الآلي(*)، والذى يمكن استخلاصه من خلال الربط بين كم الجرائم المرتكبة فى هذا النطاق وكيفية الارتكاب، ودرجة التقدم العلمي والتكنولوجي بالدولة.
- عامل فني: يتمثل في صعوبة اكتشاف جرائم الحاسب الآلي، وصعوبة ملاحقة مرتكبيها عقب تمامها.

## المطلب الأول

## التعريفات التي تناولت جرائم المعلوماتية

وفي مستهل دراسة هذا النوع الحديث من الإجرام الذى أفرزه التقدم العلمى والتكنولوجي، والتقنيات عالية المستوى المفترض تسخيرها لخدمة المجتمعات، تلقفته عقول مريضة وأنفس غير سوية، خرجت به من الجانب المفيد إلى الجانب المضر. نتعرض لدراسة علمية أكاديمية تناولت جرائم الحاسب الآلي وهى ما اصطلح على تسميتها بجرائم الكمبيوتر أو جرائم المعلوماتية، فذهبت إلى أنها:

(*) يمكن القول أنه توجد علاقة – أشبه بالعلاقة الطردية – بين كم الجرائم المعلوماتية ومستوى التقدم المعلوماتي فى الدولة، باعتبار زيادة جرائم الحاسب الآلى وارتكابها بصورة أكثر تعقيداً، كلما كانت الدولة على درجة كبيرة من التقدم العلمى والتكنولوجى، ذلك صحيح.. إذ أنه كلما كانت الدولة بعيدة بعض الشئ عن مسيرة التقدم فى بدايتها لم تبلغ حداً من التعقيد والتقنية التنفيذة المتطورة، ويمكن ملاحظة ذلك بوضوح فى نطاق الدول النامية – ان تعتمد كلياً – أو شبه كلياً – على أجهزة الحاسوب، سواء في صورتها المعقدة، بما يستبعد احتمال وجود استعمالات غير قانونية للحاسوب.

«الجـرائـم المرتبطـة بالكمـبـوتر، والتى تمثل انتـهـاكـاً للقـانون الجنائى»، ويستـوجب ارتكابها أو التـحقيق فيهـا أو المحـاكمة بشأنها دراية بالأمور الفنية للكمبيوتر[1].

وهذا الاتجاه – اجتهاد يحمد واضعه – الذى أشار إلى استلزام وجود روابط بين النشاط الإجرامى وأجهزة الحاسوب، حتى يتثلى اعتباره من جرائم الحاسب الآلى، لا يخلو من النقد، الذى تتمثل أوجه فيما يلى:

- الأطـلاق: أطلاق كلمـة (الجـرائم) الواردة فى صدر التـعـريف، وعـدم تحـديد المقصود بها.
- الخلـط: إيراد جملة (الجـرائم المرتبطة بالكمـبيـوتر)، أدخل فى عـداد جـرائم الحاسب الآلى بعضاً من الجرائم التى يتصور ارتباطها بالكمبيوتر، إلا أنها فى ذات الوقت تعـد مسـتـقلة عنه، إذ يمكن تصور وقوعـهـا بصفة منفرده ودون ارتباط بأجـهزة الحاسب الآلى. من أمثلة ذلك جرائم سرقة العلامات التجارية وتقليدهـا، إذ يمكن أن تقع السـرقة على العلامـات التـجـارية لأنواع أجـهـزة الحاسبات الآلية ذات الماركات الشهيرة من نوعية G S P, HP, LG, Apple, IBM – وفى هذه الحـالة فإن الجـريمة تعـد مرتبطة بالكمـبيـوتر، ولكنهـا لا تعكس خصائص جرائم الحاسب الآلى على النحو السابق بيانه.
- عدم الدقة في التحديد: إيراد جملة «والتى تمثل انتهاكاً للقانون الجنائى» يمثل جانب من أوجه القصور، من حيث عدم تحديد المقصود بالقانون الجنائى... **هل هو القـانون الجنائي الوطني المطبق في نطاق الدولة؟ أم القـانون الجنـائي الدولي بصفة عامة؟** ولا يخلو الأمر من النقد فى كلا الوضعين..

**في الحالة الأولي - أن المقصود هو القانون الجنائي الوطني للدولة.**

فإن التعريف يفقد سمة العمومية حيث أنه لا يصدق على كافة الدول، إذ أنه

---

(١) ورد هذا التعريف فى نشرة مركز بحوث الشرطة – (علمية – محكمة) – أكاديمية الشرطة – القاهرة – العدد الثانى – نوفمبر ١٩٩٥ – ص ٥.

من القوانين الجنائية الوطنية فى بعض الدول ما لا يحوى نصوصاً تجرم بعضاً من الأفعال غير المشروعة المرتبطة بالحاسب الآلى، وذلك مرجعه لتفسيرياً:

**الأول** - كما فى معظم البلاد النامية – دول العالم الثالث – حيث يخلو التشريع الجنائى بها من النصوص العقابية الرادعة لجرائم المعلوماتية.

**الثاني** - فى بعض البلدان يرتفع مستوى التحرر ويتشدق الجميع باطلاق مفاهيم متنوعة لمعنى الحرية البعيدة عن المعنى الحقيقى، بعض الأفعال وأن كانت غير مشروعة ومخالفة للسلوك الاجتماعى والاخلاقى، إلا أنها لا تمثل خروجاً على نظام التشريع الجنائى الداخلى لهذه الدول، فإرتكابها لا يعد جريمة يعاقب عليها القانون.. مثل جانب من الأفعال المتعقلة بالحرية الجنسية وتتمثل فى تبادل الصور والأشكال الجنسية عبر أجهزة الحاسب الآلى (ديسكات) أو عن طريق شبكة المعلومات (الإنترنت).

**وفي الحالة الثانية - أن المقصود هو القانون الجنائي الدولي.**

فإن التعريف يفقد سمة الواقعية.. باعتبار عدم اجماع الدول على ماهية الأفعال غير المشروعة المدرجة ضمن القانون الجنائى الدولى، والذى لا يعدو كونه مجرد نظرية عامة، لم يرق إلى مستوى تشريع دولى يجرم الأفعال غير المشروعة يالنسبة للجرائم المعلوماتية على مستوى المجتمع الدولى. فضلاً عن صعوبة الوصول إلى مثل ذلك لاسباب عديدة ترجع إلى اعتبارات سياسية واختلاف الثقافات والاعراف والصياغات، مع تباين الرؤية القانونية المرتبطة بالعوامل الاجتماعية والاقتصادية والدينية لكل دوالة.

- **القصور في الصياغة:** إيراد جملة (ويستوجب ارتكابها أو التحقيق فيها أو المحاكمة بشأنها دراية بالأمور الفنية للكمبيوتر)... أدخل التعريف أمراً غير متصل بماهية تلك النوعية من الجرائم. إذ أنه نظر إلى متطلبات ارتكاب أفعال معينة تعد أمور خارجة عن الماهية الدالة بصفة محضة على طبيعة

هذه الجرائم. وأنه وأن كانت الدراية الفنية بالحاسب الآلى تعد فى بادئ الأمر من الأمور العسيرة، إلا أنه مع الاتساع المطرد فى استخدام الحاسبات الآلية، أضحت أساليب التشغيل من السهولة، بحيث يكون من غير المجدى والمفيد ابرام الحديث عن الدراية الفنية للحاسب، كأساس عند تعريف الجرائم المرتبطة به.

كما أن إجراءات التحقيق والمحاكمة تعتبر مستقلة عن الجريمة وهى لاحقة على ارتكابها، ومن ثم يكون من غير المقبول تعريف الفعل بأمور لاحقة على وقوعه.

ونخلص إلى أنه إزاء التصدى لظاهرة الإجرام المعلوماتى(١)، لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول مفهوم الجريمة المعلوماتية Le de'lit Informatique. حيث ذهب جانب إلى تناولها بالتعريف على نحو ضيق، وجانب آخر عرفها على نحو متسع.

## الفرع الأول

## من التعريفات المضيقة للجرائم المعلوماتية

ما ذهب إليه الفقية (MERWE) حيث يرى أن الجريمة المعلوماتية (جريمة الحاسب) هى: «الفعل غير المشروع الذى يتورط فى ارتكابه الحاسب الآلى (AN Il Legal act where per petration involved a com puter). أو هى الفعل الإجرامى الذى يستخدم فى اقترافه الحاسب الآلى كأداة رئيسية، أو هى مختلف صور السلوك الإجرامى التى ترتكب باستخدام المعالجة الآلية للبيانات»(٢).

---

(١) كلمة معلوماتية (In formatice): هى اختصار مزجى لكلمتى معلومة Information وكلمة آلى أو آلية Automatique. ، وهى تعنى المعالجة الآلية للمعلومة. (د/ أحمد حسام طه – الجرائم الناشئة عن استخدام الحاسب الآلى [الحماية الجنائية للحاسب الآلى] – الطبعة الأولى – القاهرة – دار النهضة العربية – سنة ٢٠٠٠ – ص ٢٧٠).

(2) MERWE (Vander): "Computer crimes and other crimes against information Technology in South Africa "R.I.D.P", 1993, p. 554.

وفى رأى أخـر ذهب (Trédman) إلى أن الجـريمة المعلومـاتيـة تشـمل: «أى جريمة ضد المال، مرتبطة باستخدام المعالجة الآلية للمعلومات»(١).

فيما ذهب الفقية (ROSBL AT) إلى تعريفها بأنها: «كل نشاط غير مشروع موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب الآلى، والتى تحول طريقه».

- أو الجريمة المعلوماتية كما كما جاء فى تعريف (Dauid Tompson): «جرائم يكون متطلباً لاقترافها، أن يتوافر لدى الفاعل معرفة بتقنية الحاسب»(٢).

والحقيقة أن التعريفات السابقة للجريمة المعلومـاتية كانت قاصرة على الأحاطة بأوجه ظاهرة الإجرام المعلوماتى.

**- وعرف كلاوس تايدومان الجرائم المعلواتية بأنها:**

«كافة أشكال السلوك غير المشروع الذى يرتكب باستخدام الحاسب الآلى»(٣). ولكن يؤخذ على هذا التعريف أنه بالغ العمومية والاتساع لأنه يدخل فيه كل سلوك غير مشروع أو ضار بالمجتمع(*). وإنه غير منطقى حيث لم يبين

(1) K. Trédmann,: Fraude et autres délits d'affaires connis a l'aide d'ordinateurs électroniques, Rev, drpén. crim, 1984, p. 612.

(٢) د/ هشام رستم – جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة – بحث مقدم إلى اللجنة العلمية لأعداد التقرير الوطنى المصرى لمؤتمر الأمم المتحدة التاسع لمنع الجريمة ومعاقبة المجريمن – مجلة الدراسات القانونية – جامعة أسيوط – العدد السابع عشر – سنة ١٩٩٥ – ص ص ١٠٧، ١٠٨.

(3) Klaus Tiedeman, Fraude et eutres délits d'affaires commis a L'aide d'ordinateures électroniques, Rev. D.P.C. 1984, No. 7, p. 612.

(*) ولما كانت الجريمة بوجه عام سلوكاً ضاراً بالمجتمع أو سلوكاً غير مشروع، فكل جريمة عالجها قانون العقوبات التقليدى يمكن أن تدخل فى إطار الجرائم المعلوماتية وهذا غير معقول، فرغم أن التعريف تحفظ واستلزم أن يكون السلوك غير المشروع مرتكباً باستخدام الحاسب الآلى، إلا أن ذلك لا ينفى أنه يشمل أو يمكن أن يشمل كافة الجرائم التقليدية وهذا غير وارد.

خصوصيته ببعض الجرائم التى لا يتصور وقوعها إلا بواسطة الحاسب الآلى، فلو حدث ذلك لكان التعريف قد حدد نطاق العمومية الواردة فيه،وجعله أقرب إلى منطق التعريفات العلمية.

كما وأن مجرد استخدام الحاسب الآلى لا يضيف إلى السلوك غير المشروع جديداً، ولكن استخدام البيانات والمعلومات والبرامج هو الذى يمكن أن يضيف إلى الجريمة سمة الجريمة المعلوماتية[1].

- تعريف مكتب تقييم التقنية بالولايات المتحدة الأمريكية، حيث يعرف الجريمة المعلوماتية، من خلال تحديد مفهوم جريمة الحاسب بأنها:

«الجرائم التى تلعب فيها البيانات الكمبيوترية والبرامج المعلوماتية دوراً رئيسياً»[2].

وهذا التعريف أيضاً ليس بمنأى عن النقد، حيث أنه يعرف الجرائم المعلوماتية بأنها الجرائم، وهذا من قبيل تفسير الشئ بالشئ، كما وأنه لا يحدد طبيعة الجريمة المعلوماتية وإن كان قد خطى خطوة معقولة عندما بين أن البيانات الكمبيوترية والبرامج المعلوماتية تلعب فيها دوراً رئيسياً.

- وعرف Leslie D. Ball الجريمة المرتبطة بالحاسب بأنها:

«فعل إجرامى يستخدم الحاسب فى ارتكابه كأداة رئيسية». ولكن هذا التعريف تعرض للنقد أيضاً – كما تعرض تعريف كلاوس تايدمان – حيث أن التعريفات التى ترتكز على وسيلة ارتكاب الجريمة ليست جامعة ولا مانعة كما

---

(١) محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلى – دار الجامعة الجديدة – الاسكندرية – سنة ٢٠٠١ – ص ٧٢.

(2) Adressing the New Hazards of the High tecknology Workplace, Harvard Law review, vol - 104, No, 8, Juin 1991, Notes, p. 1998 Cited by Dr. Hesham Rastom. p. 30.

أنها تتسم بقصور كبير فى إعطاء تصور علمىٍ للجرائم المعلوماتية، ومنها الجرائم التى تقع على برامج الحاسب الآلى. وذهب رأى فى نقد هذه التعريفات إلى أن الاعتماد فى تعريف الجريمة المعلوماتية على الوسيلة المستخدمة فى ارتكابها يواجه تقييم مفاده أنه لكى نعرف الجريمة يجب الرجوع إلى العمل الأساسى المكون لها، وليس فقط إلى الوسائل المستخدمة لتحقيقها، فليس لمجرد أن الحاسب قد استخدم فى جريمة فإنه يجب اعتبارها من الجرائم المعلوماتية. ولذا قد يكون من أفضل التعريفات التى تدور حول الوسيلة هو تعريفها بأنها: «تلك الجرائم التى يكون قد وقع فى مراحل ارتكابها بعض عمليات فعلية داخل نظام الحاسب، أى أنها الجرائم التى يكون دور الحاسب فيها إيجابياً أكثر منه سلبى»[1].

وفى تعريف أخر لجريمة الحاسب بأنها: «نشاط غير مشروع، موجه لنسخ أو تغيير أو حذف أو الوصول إلى المعلومات المخزنة داخل الحاسب، أو التى تحول عن طريقه»[2].

---

(١) دكتور/ هشام محمد فريد رستم – مرجع سابق، ص ص ٣٠ ، ٣١.

وقد ذهب إلى تأييد التعريف البلجيكى القائل بأن الجريمة المعلوماتية هى: «كل فعل أو امتناع من شأنه الاعتداء على الأموال المادية أو المعنوية، يكون ناتجاً بطريقة مباشرة أو غير مباشرة عن تدخل التقنية المعلوماتية». (المرجع السابق – ص٣٣).

(٢) تعريف روز بنلات ورد فى مرجع:

- Alexander (Michael): Computer crime. Ugly secret for business, Computer World, Vol. xxiv, No, 11, March, 21, 1990, p. 104.

وأن كان هذا التعريف يتسم بقدر من التكامل غير المتوافر للتعريفات السابقة، إلا أنه يلاحظ عليه:

- بدأ التعريف صائباً وانتهى معيباً، فقد بين أن جريمة الحاسب الألى تعتبر من الجرائم المحصورة لا تلك التى لا تقع تحت حصر، فحقق بذلك أساس فكرة المشروعية – أنه لا جريمة بغير نص – ولكنه أنتهى إلى توسع غير مبرر فى التعريف حيث ذكر أن جريمة الحاسب يمكن أن تنتج من أى نشاط غير مشروع يتعلق بالمعلومات التى يمكن أن تحول عن طريقه، فلم يبين طبيعة هذا التحويل ففتح الباب واسعاً أمام التفسيرات التى يمكن أن تعصف بمبدأ المشروعية.
- أن التعريف لم يبين محل الاعتداء، رغم أنه تعريف يدرج عادة تحت تقسيم التعريفات المتركزة حول موضوع الجريمة (محمد محمد شتا – مرجع سابق – ص ٧٤).

-/-

وإزاء هذه الانتقادات(1)، حاول جانب من الفقه تعريف الجريمة المعلوماتية على نحو واسع في محاولة لتفادى أوجه القصور التي شابت تعريفات الاتجاه المضيق في التصدى لظاهرة الإجرام المعلوماتي(2).

## الفرع الثاني

## من التعريفات الموسعة لمفهوم الجريمة المعلوماتية(3)

ما ذهب إليه الفقيهان (MICHEL & CREDO) من أن سوء استخدام الحاسب Computer Abuse أو جريمة الحاسب Computer Crime تشمل:

---

= والذى ذهب إلى أن الجريمة المعلوماتية هي سلوك إجرامي ايجابي أو سلبي، من شأنه الاعتداء بأي صورة من الصور، على المعلومات أو البيانات المخزنة داخل الحاسب أو داخل وسائط أخرى يتم تخزين المعلومات فيها من خلاله على نحو يلحق ضرراً فعلياً أو مفترضا بالجهة التي تم تخزين المعلومات لمصلحتها.

(1) بعض الفقهاء عند تناولهم لتعريف الجريمة المعلوماتية كان تركيزهم على موضوع الجريمة، وركز البعض الآخر على وسيلة ارتكابها، بينما ذهب البعض الآخر إلى التركيز على فاعل الجريمة.
- M. Masse: La droit penal special né de I'informatique in ibformatique et droit pénal travaux de I'institut de sciences criminelles de poietiers 1981 - 4 éd cujas. p. 23.

(2) وفي تسميات أخرى للجريمة المعلوماتية بأنها: جريمة الحاسب الآلي، أو جريمة إساءة استخدام الحاسب، أو الجريمة المتعلقة بالحاسب، أو الجريمة المتعالجة للبيانات، بل أن هناك من طلق عليها جريمة الغش المعلوماتي، أو الاحتيال المعلوماتي، أو الاختلاس من المعلوماتي. للمزيد في هذا الشأن يراجع:
دكتور/ هلالى عبد اللاه أحمد - التزام الشاهد بالأعلام في الجرائم المعلوماتية (دراسة مقارنة) طبعة أولى - القاهرة - دار النهضة العربية - سنة ٢٠٠٠، د/ محمد حسام لطفي - الحماية القانونية لبرامج الحاسب الآلي الأليكتروني - دار الثقافة للطباعة والنشر - القاهرة - سنة ١٩٨٧، دكتور/ على عبد القادر القهوجي - الحماية الجنائية لبرامج الحاسب الآلي - الطبعة الأولى - القاهرة - دار الحاسب للطباعة والنشر - سنة ١٩٩٩، د/ هدى حامد قشقوش - جرائم الحاسب الالكتروني في التشريع المقارن - الطبعة الأولى - القاهرة دار النهضة العربية - سنة ١٩٩٢، د/ محمد أمين أحمد - جرائم الحاسوب والأنترنت - مرجع سابق - سنة ٢٠٠٤.

(3) د/ هلالى عبد اللاه أحمد - تفتيش نظم الحاسب الآلي وضمانات المتهم المعلوماتي (دراسة مقارنة) - القاهرة - دار النهضة العربية - سنة ٢٠٠٠ - ص ١٠٥ وما بعدها.

«استخدام الحاسب كأداة لارتكاب الجريمة.... As a tool in the perpetration of a crime هذا بالإضافة إلى الحالات المتعلقة بالولوج غير المصرح به لحاسب المجنى عليه أو بياناته، كما تمتد جريمة الحاسب لتشمل الاعتداءات المادية سواء على جهاز الحاسب ذاته أو المعدلات المتصلة به، وكذلك الاستخدام غير المشروع لبطاقات الائتمان Credit Carts، وانتهاك ماكينات الحساب الآلية، بما تتضمنه من شبكات تحويل الحسابات المالية بطرق الكترونية، وتزييف Counterfeit المكونات المادية والمعنوية للحاسب، بل وسرقة جهاز الحاسب فى حد ذاته أو أى مكون من مكوناته.

* وتناول رأى من الفقه تعريف الجريمة المعلوماتية بأنها: (عمل أو امتناع يأتيه الإنسان أضراراً بمكونات الحاسب وشبكات الاتصال الخاصة به، التى يحميها قانون العقوبات ويفرض له عقاباً) (*).

**ويمتاز هذا التعريف بالسمات التالية:**

١- أنه يحتوى على كل صور الاعتداء الإيجابية أو السلبية التى تقع أضراراً بمكونات الحاسب المادية والمعنوية وشبكات الاتصال الخاصة به، باعتبارها من المصالح والقيم المتطورة التى تمتد مظلة قانون العقوبات لحمايتها.

٢- أنه يتضمن الأثر الجنائى المترتب على العمل أو الامتناع غير المشروعين، ويتمثل فى الجزاء الجنائى بكافة صوره وأنواعه، وهو أشد أشكال التعبير عن معنى الإلزام فى القاعدة القانونية.

٣- أنه يحافظ على الشرعية الجنائية "Nulum crimena mulla poena sine

(*) رأى د/ هلالى عبد اللاه أحمد: حيث قام بصياغته مستوحياً أياه من تعريف الجريمة التقليدية بأنها: «عمل أو امتناع يأتيه الإنسان إضراراً بمصلحة حماها المشرع فى قانون العقوبات، ويترتب عليه أثر جنائى يتمثل فى العقوبة أو التدبير الاحترازى»، للمزيد يراجع مؤلف د/ هلالى عبد اللاه أحمد - شرح قانون العقوبات (القسم العام) - القاهرة - دار النهضة العربية - سنة ١٩٨٨، ص ٣٦.

"lege : وتعنى أنه لا جريمة ولا عقوبة إلا بنص، إذا لا يمكن أن يوجه أى اتهام ضد شخص لإرتكابه فعلاً معيناً ما لم يكن منصوصاً على تجريم هذا الفعل فى القانون، كما لا يمكن تطبيق عقوبة ما لم تكن محدودة سلفاً(١).

ومؤدى هذه السمة الأخيرة أن يحدد قانون العقوبات مقدماً الأفعال التى تعتبر جرائم معلوماتية والعقوبات المقررة لهذه الجرائم المعلوماتية، ونظراً لخطورة هذه الجريمة وآثارها الممتدة التى قد تصل من دولة إلى أخرى، فإن بعض الهيئات الدولية المعنية بجرائم الكمبيوتر قد أرست قواعد لتعريف هذا النوع من الجرائم، من هذه الهيئات الـ (OECD)(٢) التى اتخذت التعريف التالى كتعريف عملى لجريمة الكمبيوتر أو الجريمة المتعلقة بالكمبيوتر: أى سلوك غير قانونى أو غير أخلاقى أو غير مفوض يتعلق بالنقل أو المعالجة الآلية للبيانات يعتبر اعتداء على الكمبيوتر(٣).

وقد اقترحت جماعة الخبراء لهيئة (OECD) بتصنيف وظيفى بحيث يسرد - يحدد - النشاطات التى يجب أن تطبق عليها العقوبة الجنائية(٤)، بينما لم يحاول المجلس الأوربى فى تقريره الذى أعده عام ١٩٩٠م إيجاد تعريف رسمى لجريمة الكمبيوتر وترك ذلك لأعضاء كل دولة لاقتراح التصنيف الوظائفى بما يلائم أنظمتها القانونية الخاصة بها.

---

(١) لمزيد من التفصيل حول مبدأ الشرعية الجنائية بوجه خاص يراجع:

* BENL ATRCHE (Abdelouahab): "Le Pricipe de la légalité criminelle: Etude de droit comparé Thése poitiers 1981.

(٢) هى هيئة التعاون الاقتصادى والتنمية.

(3) htt: / 10.10.1.2/Team/magazine 2/OL D% 20 magazin / andyal / Taareef. htm 27/1/2002.

(٤) عرف أحد الخبراء جريمة الكمبيوتر بأنها: (أى عمل غير مشروع يؤخذ فيه الكمبيوتر أداة أو هدف)، وخبير آخر عرفها بأنها: (أى حادثة تعضدها تكنولوجيا الكمبيوتر وفيها يتحمل أو قد يتحمل ضحيتها خسارة، ويكون مرتكبها عن قصد أو قد يحقق بها مكسب).

* D.B. Parker: Comibattre La criminalité informatique, édoros 1987,p.18.

• وبعد أن عرضنا لتعريف الجريمة المعلوماتية نضيف: أن شبكة الإنترنت – بوصفها نتاج تطور النظم المعلوماتية – كأداة للربط والاتصال بين مختلف شعوب العالم، تشكل أداة لارتكاب الجريمة المعلوماتية أو محلاً لها، وذلك بإساءة استخدمها أو استغلالها على نحو غير مشروع، وتعد الجرائم المرتكبة غير شبكات الإنترنت من الموضوعات الحديثة الهامة، التى فرضت تواجدها على مستوى الدول محلياً والعالم دولياً.

ولذلك ينبغي على الجهات التشريعية – وبخاصة المشرع الجنائي، إقليمياً ودولياً – مواجهتها بتشريعات حاسمة لمكافحتها وتقديم مرتكبها للعدالة(١).

ومن صور الجريمة المنظمة على شبكة الانترنت ما عرف بالإرهاب الإليكترونى E- Terrorism وأيضا جريمة غسل الأموال عن طريق تحويلها، أو

---

(١) الإنترنت: عبارة عن شبكة تتألف من العديد من الحاسبات الآلية المرتبطة ببعضها البعض، إما عن طريق الأقمار الصناعية، وتمتد عبر العالم لتولف فى النهاية شبكة هائلة، بحيث يمكن للمستخدم لها User الدخول إليها من أى مكان وفى أى وقت، طالما كان جهاز الحاسب الآلى مزدواً بموديوم Modem يربطه بخط الهاتف لتلقى وإرسال البيانات عبر مزود الخدمة Service Provider. (د/ جميل عبد الباقى الصغير – الانترنت والقانون الجنائى «الأحكام الموضوعية للجرائم المتعلقة بالانترنت») – دار النهضة العربية – القاهرة – ط أولى – سنة ٢٠٠١ – ص ٤.

ويراجع بشأن تاريخ الإنترنت: بيل جيتس – المعلوماتية بعد الإنترنت – ترجمة: عبد السلام رضوان – إصدارات المركز الوطنى للثقافة – سلسلة كتب ثقافية شهرية – الكويت – سنة ١٩٩٨.

* VINIG. Cerf and Robert E. Kahn: Abrife History of The internet and Related Networks. Version 31-3-2000, at http: // www. info. isoc. org/ guest/ zakon/ internet History / Brief - history - of - The - internet.

* والإنترنت كلمة إنجليزية الأصل وهى اختصار مزجى للحروف الأولى من كلمتى International بمعنى دولى وكلمة Network بمعنى شبكة، وقد ظهر أول ربط بين الحاسب وأجهزة الاتصال فى عام ١٩٤٠م، إلى أن أصبحت الحاسبات الشخصية P.C.S تستطيع الارتباط بشبكات الآت أتصال والاستفادة من المعلومات المخزنة والمتبادلة عبر خطوط الاتصال.

(راشد عايض المرى – مدى حجية الوسائل التكنولوجية الحديثة فى إثبات العقود التجارية – رسالة مقدمة لنيل درجة الدكتوراة – كلية الحقوق – جامعة القاهرة – القاهرة – سنة ١٩٩٨ – ص ٣١.

إجراء عمليات معقدة من التحويلات النقدية عبر الإنترنت من حساب لآخر، لإخفاء الصفة غير المشروعة لمصدر الأموال القذرة.

## الفرع الثالث

## التمييز بين جرائم الحاسب الآلي وجرائم الإنترنت في نطاق الجريمة المعلوماتية

ظهرت جرائم الإنترنت فى وسط الجرائم الحديثة ذات التقنية العالمية فى نهاية الثمانينات من القرن المنصرم، وكان ظهورها من خلال أطلاق جرائم العدوان الفيروسى، جريمة دودة موريس المؤرخة واقعتها فى نوفمبر ١٩٨٨(*).

وقد أطلقت المحافل الدولية والمؤتمرات المعلوماتية مصطلح جرائم الإنترنت، فى مؤتمر جرائم الإنترنت، المنعقد فى أستراليا الفترة من ١٦-١٧ فبراير ١٩٩٨.

وللوقوف على عناصر التمييز بين جرائم الحاسب وجرائم الإنترنت نفضل أن نبدأ بالتعريف، فتقابلنا حقيقة هامة هى أن مسألة تعريف جرائم الإنترنت من المسائل الشائكة التى تقف كحجر عثر أمام الفقه، إذ أنه وحتى الآن يصعب وضع تعريف عام وشامل لها(**).

---

(*) تتلخص وقائع القضية فى أن المدعو/ موريس قام بتصميم دودة، وأدين نتيجة لذلك بتهمة انتهاك القانون الصادر عام ١٩٨٦ والمتعلق بالاحتيال وسوء الاستخدام فى مجال الكمبيوتر، وعوقب بالسجن لمدة ٣ سنوات مع وقف التنفيذ وإيقافه تحت المراقبة وغرامة عشرة آلاف دولار.

(**) ذلك ما أكدته قمة برلين.. بنصها التالى:

- Le Sommet de Berlin, relaif à La cybercriminalité n'aura Permis de dégager qu'une seule certitude, it est Pour L'instant impossible de s'accorder sure une délinition universel de la cybercrimina lité et L'on Peut méme se demandé si une entente sera un Jour Possible.
  Cybercriminalité, 17 décembre 2004, disponible en ligne à l'adresse suivante: http: // www. assemblee - Nationale. fr.

=/=

فهناك من ذهب إلى أن جرائم الإنترنت هي: «أي جريمة يمكن ارتكابها بواسطة نظام حاسوبي أو شبكة حاسوبية، أو داخل نظام حاسوب. وتشمل تلك الجريمة من الناحية المبدئية جميع الجرائم التي يمكن ارتكابها في البيئة الإلكترونية»[1]. أو بأنها: «كل اعتداء يقع على نظم الحاسب الآلي وشبكاته أو بواسطتها»[2].

وفي هذا السياق تجدر الإشارة إلى أن الكثير من الباحثين في مضمار الجرائم ذات التقنية الحديثة يستخدمون مصطلحات غير دقيقة للتعبير عن جرائم الإنترنت، إذ إننا نجد البعض يستخدم مصطلح (الإجرام المعلوماتي) La crimina Lité Informatique أو Ledélinquance informatique، أو يستخدم مصطلح (جرائم التكنولوجيا المتقدمة) La criminalité de haute technologie، أو مصطلح (الغش المعلوماتي).

في حين أنه يجب استخدام المصطلح الدقيق المعبر عن طبيعة تلك الجرائم وهو (جرائم الإنترنت)، ذلك لأن (الإجرام المعلوماتي) وإن كان يقصد به التعبير عن الجرائم الواقعة عن طريق جهاز الكمبيوتر، إلا أن هذا لا يعني من جهة أخرى أن الاعتداء على المعلومة يتحقق دائماً باستخدام الكمبيوتر وخصوصاً باستخدام تلك الجريمة، وبالتالي فالجريمة المعلوماتية قد تكون أشمل من جرائم الإنترنت، وذات الشأن بالنسبة (للغش المعلومات) وجرائم (التكنولوجيا المتقدمة)[3].

---

= مشار إليه لدى، نبيلة هبة هروال - الجوانب الإجرائية لجرائم الإنترنت (في مرحلة جمع الاستدلالات) - دار الفكر الجامعي - الإسكندرية - سنة ٢٠٠٦ - هامش (٢) - ص ٢٤.

(١) التعريف الذي تبناه مؤتمر الأمم المتحدة العاشر لمنع الجريمة ومعاملة المجرمين المنعقد في فيينا الفترة من ١٠-١٧ أبريل ٢٠٠٠.

(٢) محمد أمين أحمد الشوابكة - جرائم الحاسوب والإنترنت - مرجع سابق - ص ١٠.

(٣) نبيلة هبة هروال - المرجع السابق - ص ٣١.

ونحن نؤيدها فيما ذهبت إليه، حيث أن جرائم الإنترنت تعد من أصناف الجريمة المعلوماتية، =/=

أ - أوجه التشابه:

تختلف جريمة الإنترنت عن جريمة الحاسب الألى فى أوجه متعددة، إلا أنه من الأفضل قبل عرض هذا الاختلاف، الاشارة إلى بعض أوجه التشابه المشتركة بين الجريمتين .. والتى منها:

- تعد جريمة الإنترنت وجريمة الحاسوب من الجرائم الخطيرة، ذات الآثار الوخيمة، فهما من ذات صنف جرائم التقنية الحديثة، وقد تتعدى نتائج أى منهما المستوى الشخصى لفرد إلى مستوى منظمة أو هيئة أو كيان اقتصادى أو سياسى.
- المجرم المعلوماتى فى كلا منهما يتمتع بصفات وسمات عالية، ويختلف عن المجرم التقليدى، وهو ذو دراية وعلم ومعرفة متقدمة بالأنظمة المشغلة لكليهما، سواء الإنترنت أو الحاسوب.
- كلا من الجريمتين تشتركان فى أن أداة ارتكاب أى منهما هى (جهاز الحاسب الآلى).
- كما تشترك جرائم الإنترنت وجرائم الحاسب فى صعوبة الاكتشاف،واتباع ذات طرق الإثبات الجنائى لضبط الفاعل.

---

-- التى تتنوع وتتزايد أشكالها مع التقدمات التقنية المستحدثة.

كما وأنه على المستوى الدولى تضمن مؤتمر القانون والإنترنت المنعقد فى لشبونة/البرتغال الفترة من ٢٦-٢٧ يناير ٢٠٠١، أنه يجب عدم الالتفات إلى مثل هذه المصطلحات غير الدقيقة، وإعتماد مصطلح (Cyber Crime) دون غيره للتعبير عن جرائم الإنترنت، مع الأخذ فى الإعتبار التمييز بين الجرائم التى يمكن ارتكابها عبر الإنترنت، وتلك التى لا يمكن ارتكابها عبر تلك الأخيرة. (دكتور/ عمر محمد أبو بكرين يونس – الجرائم الناشئة عن استخدام الإنترنت – دار النهضة العربية – القاهرة – سنة ٢٠٠٤ – ص ١٥٨)

ب- أوجه الاختلاف[1]:

- الوسيلة: جريمة الحاسب (سواء أكان وسيلة أم معتدى عليه) يمكن أن تتم دون الحاجة إلى الارتباط بشبكة الإنترنت، مثل توظيف الحاسبات وملحقاتها في جرائم التزوير والتزييف أو سرقة المعلومات وتدميرها.

أما جريمة الإنترنت فشرطها الرئيسي وجود جهاز حاسب الآلي متصل بالإنترنت لإتمام أركانها(*).

- بدء الظهور: تاريخياً أرجع الفقه الجنائي ظهور جرائم الحاسب الآلي إلى عام ١٩٦٠، أما جرائم الإنترنت فيرجعها إلى العام الذي أفاق فيه العالم على دودة موريس عام ١٩٨٨. والتي كانت السبب في تعديل التشريع الفيدرالي الأمريكي.
- شخص الجاني: مجرم الإنترنت المميز هو الهاكر، الذي يتخذ الشكل الخبيث له في مصطلح الفقيه الايطالي كرارا (Carrara). في حين أن مجرم الحاسب الآلي هو القرصان مرتكب جرائم العدوان على حقوق الملكية الأدبية والفكرية عامة، وجرائم استخدام التقنية الحديثة للسيطرة على تشغيل الحاسوب،خاصة اختراق كلمات العبور لملفات مشفرة مخزنة في الحاسوب.

وتجدر الإشارة إلى أنه يُطلق على الهاكر في الدراسات العربية مصطلح القرصان أو المخترق (**).

ويختلف مجرم الإنترنت عن مجرم الحاسب الآلي في كونه مجرماً لا يتمتع بمدارك علمية أو تخصصية ذات طابع أكاديمي، وإنما هو يملك تقنية الإنترنت دون حاجة لأن يكون دارساً لها، ولعل أفضل دليل على ذلك ا لأطفال (الأحداث) الذين يرتكبون تلك الجرائم وهم مايزالون في سن مبكرة.

---

(١) نبيلة هبة هروال – المرجع السابق – ص ٥٤ وما بعدها.

(*) بالرغم من استعمال الإنترنت عبر الهاتف، والهاتف الخلوي إلا أن ذلك لا يعني عدم اعتماده على الحاسوب، إذ أن الهاتف الخلوي ما هو إلا تقنية حديثة من تقنيات الحوسبة المتطورة.

(**) انظر التمييز بين الهاكرز والقرصان بتوسع في الجزء الثاني من الدراسة، ص ٥٤٥.

كما يرتبط سلوك مجرم الإنترنت بظاهرة الاختراق، عكس مجرم الحاسب الآلى الذى يرتبط بالقرصنة[1].

- القانون المنظم: الإنترنت يحكمه قانون الإنترنت(*)، على عكس الحاسوب الذى يحكمه قانون الحاسوب.

- التقنية الإجرامية: اختلاف فيروس الإنترنت كجريمة تقلدية عن فيروس الحاسب الآلى، ذلك لأن فيروس الحاسب برز لأول مرة سنة ١٩٧٤ فى شركة (Terot) على عكس فيروس الإنترنت الذى ظهر سنة ١٩٨٨.

هذا من جهة.. ومن جهة أخرى يتميز فيروس الإنترنت بأنه سريع الانتشار طالما أن الشبكة تعمل، وحتى لو أغلق أحد الحواسيب أو الشبكات أو الخوادم، أضف إلى ذلك أن مهام ذلك الفيروس – الإنترنتى – تتجاوز عملية التخريب، إذ يمكن استخدامه فى الاختلاس المعلوماتى.

مثال ذلك ما كشف عنه التطور الفيروسى عن وجود دودة يطلق عليها Badtrans, 13312 @ mm تلعب دوراً المختلس المعلوماتى، الذى يختلس النظام المعلوماتى وما يحويه من معلومات مخزنة.

بينما فيروس الحاسوب يكمن فى الحاسوب المصاب به ولا ينتقل إلى حاسبات أخرى إلا عند انتقال ملف أو برمجة من الحاسوب المصاب إلى الحاسوب غير المصاب.

أضف إلى ذلك أن فيروس الإنترنت لا يلزمه تدخل إنسانى للانتشار، على عكس فيروس الحاسب.

---

(١) للمزيد من التفاصيل فى هذا الشأن يراجع:
د/ عمر محمد أبو بكرين يونس – المرجع السابق – ص ٢٣٢ وما بعدها.

(*) قانون الإنترنت (Cyber Law): هو نوع جديد من فروع القانون، وهو يجمع فى علاقة واحدة مباشرة بين معالجة البيانات والمعلوماتية وبين خدمات الاتصال.
ومن أمثلة ذلك القانون رقم ١٥ لسنة ٢٠٠٥ بشأن تنظيم التوقيع الالكترونى، والذى ورد فى مادته الثالثة أن الهيئة – هيئة تنمية صناعة تكنولوجيا المعلومات (المناط بها تنفيذ نصوص القانون) – تهدف إلى تحقيق أغراض تشجيع وتنمية صناعة تكنولوجيا المعلومات والاتصالات.

## المطلب الثاني

## خصائص الجريمة المعلوماتية

الجريمة المعلوماتية افراز ونتاج لتقنية المعلومات، واتساع نطاق تطبيقها فى المجتمع، مما يعطيها لوناً أو طابعاً قانونياً خاصاً(*). ويميزها بمجموعة مشتركة من الخصائص يمكن تجميعه حول المحاور التالية(١):

**أولاً: الهدف (الدافع) على الارتكاب:**

تستهدف أكثر الجرائم المعلوماتية ادخال تعديل على عناصر الذمة المالية. ويكون الطمع – الذى يشبعه الاستيلاء على المال – دافعها. وبريق المكسب السريع محركها. وقد ترتكب أحياناً لمجرد قهر نظام الحاسب وتخطى حواجز الحماية المضروبة حوله(**). أو بدافع الانتقام من رب العمل أو أحد الزملاء.

---

(*) هذا ما عناه بيلفون Bellefonds بقوله أن: «الجريمة المعلوماتية حقيقة اجتماعية مميزة، تنزع لأن تصبح كذلك فئة أو صنفاً قانونياً خاصاً».

- X. Linant Bellefonds. L'informatique et le droit, Paris, 1981, p. 68.

(١) د/ هشام رستم – مرجع سابق – ص ٣٨ وما بعدها.

مشيراً إلى أن خصائص الجرائم المعلوماتية، والسمات العامة لمرتكبيها مستمدة بشكل أساسى من:

- Harold Joseph Highland, Protecting your Microcomp uter system. John wiley & Sons, INC, 1984, pp. 12-13. Marc Jaeger, La fraude informatique, R.D. P.C. Avril 1985, pp. 331-338. Bill Zalud. Computer Criminals will be Prosecuted. Adopting a'Preventing fires.†ättittud ', Data Management, April 1983, pp. 30-31.

(**) أظهرت دراسة أجرتها جمعية المحامين الأمريكيين The American Bar Association حول إساءة استخدام الحاسب أن تحقيق الكسب المالى هو السبب الأول شيوعاً وراء اتيانه، وأن التحدى الذهنى Intellectual challenge هو الشائع الثانى الذى يقف ورائه، وأن معظم من يسيئون استخدام الحاسب (٧٧٪) يكونون من داخل المنظمة (المجنى عليها)، وأن معدل الخسارة المالية الناجمة عن الحالة الواحدة لإساءة استخدام الحاسب تتراوح بين ٢–١٠ مليون دولار للمزيد بشأن نتائج هذه الدراسة يراجع:

- Bernard P. Zajac. What to Do When you lave Reason to Believe your computer has been compromised, computers & security, vol. 5 No.1, March 1986, pp. 11-12.

ويستهدف السلوك الإجرامي في الجريمة المعلوماتية معنويات وليس ماديات محسوسة، ولذلك يثار في هذا النطاق مشكلات الاعتراف بحماية المال المعلوماتي، حيث تنطوي هذه الجرائم على سلوكيات غير مألوفة، نتج عنها خسائر مادية كبيرة قياساً بالجرائم التقليدية، كما اتاحت الجرائم المعلوماتية تسهيل ارتكاب جرائم أخرى لتحصيل المكاسب المادية، جعلت حتى ملاحقة الجرائم التقليدية أمراً صعباً متى تم ارتكابها باستخدام النظام المعلوماتي.

- **ازدواجية محل الجريمة:**

نظراً لأن النظام المعلوماتي ذاته ليس من طبيعة واحدة فهو يتكون من عناصر مادية وأخرى غير مادية، بما يسمح بإمكانية أن يكون موضوع الجريمة ذا طبيعتين مختلفتين، أحدهما يتمثل في الجانب المادي، والآخر يتمثل في جانب غير مادي، وذلك ليس على مكونات النظام ذاته بل يشمل ظهور المحل الواحد بمظهرين أحدهما مادي والآخر غير مادي، كما هو الحال بالنسبة للمعلومات:

- فقد تكون في حالة انتقال أو موجودة في ذاكرة النظام المعلوماتي،أي أنها في حالة (غير مادية).
- أو تكون تلك المعلومات متجسدة (في صورة مادية)، يتخز بينها على دعامة معلوماتية.

حتى أن المعلومات بطبيعتها غير المادية يمكن أن تخضع لأكثر من نص قانوني، وفقاً لما إذا كانت في شكل مادي أو غير مادي، وفي الشكل الآخير يوجد لها أكثر من نص قانوني يمكن أن تخضع له، مثال ذلك اعتبارها مصنف أدبي، مما يوجد مشكلة تعدد الأوصاف القانونية على ذات المحل(*).

---

(*) يعبر أحد الفقهاء عن ذلك – التحول من المادية إلى اللامادية في مجال الجريمة المعلوماتية – بقوله بأنه يشاهد في ظل المعلوماتية عملية تطويق وانحسار للسلوكيات المادية، ويلاحظ ذلك الأمر في العلاقة بين الأفراد وانقطاع الاتصال المادي فيما بين الجاني والمجني عليه، وكذلك
=/=

ثانياً: موضوعها بالنسبة لمراحل تشغيل نظام المعالجة الآلية للبيانات:

بالرغم من إمكانية ارتكاب الجرائم المعلوماتية أثناء أية مرحلة من المراحل الأساسية لتشغيل نظام المعالجة الآلية للبيانات (الإدخال – المعالجة – الاخراج)، فإن لكل مرحلة منها نوعية خاصة من الجرائم لا يمكن – بالنظر لطبيعتها – ارتكابها إلا فى وقت محدد يعتبر – بالنسبة لمراحل التشغيل – الأمثل لذلك(*).

- ففي مرحلة المدخلات:

حيث تترجم المعلومات إلى لغة مفهومة من قبل الحاسب، يسهل ادخال معلومات غير صحيحة وعدم ادخال وثائق اساسية Documents - Clés. وفى هذه المرحلة يرتكب الجانب الأكبر من الجرائم المعلوماتية.

- وفي مرحلة المعالجة:

يمكن ادخال أية تعديلات تحقق الهدف الإجرامى عن طريق التلاعب فى برامج الحاسب، كدس تعليمات غير مصرح بها فيها، أو تشغيل برامج جديدة تلغى – كلياً أو جزئياً – عمل البرامج الأصلية.

---

— فى محل الجريمة يتحول موضوعها من النطاق المادى إلى النطاق غير المادى الذى يتناسب مع البيئة المعلوماتية، فالطابع الإلكترونى يكون هو المسيطر على التعامل وإتمام المعاملات المختلفة.

- Pradel (J.), Conclusion du colloque sur L'informatique et Droit Pénal, Paris, Cujas, 1983, p. 155.

(*) قد يصعب تصور حدوث الجرائم التى تقع على البرامج فى كل هذه المراحل، ولكن الدراسات المتأنية تؤكد ذلك. فالنسبة لمرحلة الأدخال يمكن أن يحدث تواطؤ بين المدخل وبين من يتم الاعتداء لحسابه، فيتم إدخال معلومات غير صحيحة تضر بأصحاب المؤسسات المعتدى عليها، بينما يتم أعطاء المعلومات الصحيحة لمن يحصل على هذه البرامج لكى يعيد بعد ذلك إدخالها وإحلالها محل المعلومات غير الصحيحة، فيصعب إثبات أن البرنامج قد تم الاعتداء عليه، لأن المعتدى يستطيع أن يدفع بحدوث تحوير Transpositions فى البرنامج، على نحو يقطع الصلة بين البرنامج الجديد والمؤسسة التى كان ينتمى إليها، فتعد تلك مسألة إثبات،وفى مرحلة المعالجة حيث يتم إدخال تعديلات تحدث نوع من التلاعب فى البرامج، وهو تلاعب يضر بالمؤسسة التى ينتمى البرنامج إليها. وفى مرحلة المخرجات يكون الاعتداء على البرامج من خلال التلاعب فى النتائج التى يجريها الحاسب ويخرجها وذلك رغم صحتها فى الادخال والمعالجة (محمد محمد شتا – مرجع سابق – ص ١٠٠).

والجرائم المرتكبة فى هذه المرحلة تتطلب توافر معرفة فنية عميقة لدى الفاعل، واكتشافها صعب، وغالباً ما تقف المصادفة وراء اكتشافها.

- وفي المرحلة الأخيرة المتعلقة بالمخرجات:

يقع التلاعب فى النتائج التى يخرجها الحاسب بشأن بيانات صحيحة أُدخلت فيه،وعالجها بطريقة صحيحة.

**ثالثاً: التعاون والتواطؤ علي الإضرار:**

هو أكثر تكراراً فى الجرائم المعلوماتية عنه فى الأنماط الأخرى للجرائم الخاصة،أو جرائم أصحاب الياقات البيضاء. وغالباً ما يكون متضمنا فيها متخصص فى الحاسبات، يقوم بالجانب الفنى من المشروع الإجرامى، وشخص آخر من المحيط أو من خارج المؤسسة (المجنى عليها) لتغطية عملية التلاعب وتحويل المكاسب إليه، كما أن من عادة من يمارس التلصص على الحاسبات تبادل المعلومات بصفة منتظمة حول أنشطتهم.

**رابعاً: دور المخالطة الفارقة:**

تتبدى فى الجرائم المعلوماتية أعراض المخالطة الفارقة The differential association syndrome بشكل ملحوظ نظراً لانتشار أنواع خاصة من الممارسات والعمليات غير المشروعة فى ميادين استخدام المعالجة الآلية للبيانات، واعتبار بعضها من قبيل الانحراف المقبول فى هذه الميادين، مما يتيح وييسر إقدام العاملين فيها على ارتكاب أفعال غير مشروعة قد تصل إلى حد الجرائم الخطيرة. فضلاً عن أن الطبيعة التنافسية لعمل المخصصين فى الحاسبات ومراكزهم المرموقة – غالباً – يمكن أن تؤدى إلى نوع من الإثارة والمزاحمة بينهم فى ارتكاب الجرائم المعلوماتية.

**خامساً: أعراض النخبة:**

يعتقد بعض المتخصصين فى تقنية الحاسبات والمعلوماتية أن من مزايا مراكزهم الوظيفية ومهاراتهم الفنية،استخدام الحاسبات وبرامجها لأغراض

شخصية، أو للتبارى الفكرى فيما بينهم، أو ممارسة بعض الهوايات الرائدة فى فلك هذه التقنية، وهو ما يعبر عنه بأعراض النخبة Syndrome clitiste. ومن شأن ذلك تمادى بعضهم إلى استخدام نظم الحاسب بصورة غير مشروعة،تصل إلى حد ارتكاب الجرائم الخطيرة.

فالملاحظ أن الصورة التقليدية للمجرم تكاد تختفى فى جرائم المعلوماتية، بل على العكس من ذلك فإن المجرم المعلوماتى عادة ما يكون على قدر كبير من العلم، كما أنه ينتمى إلى مستوى اجتماعى مرتفع نسبياً عن غيره من ذوى النشاط الإجرامى. ومن ناحية أخرى يندر أن يكون المجرم المعلوماتى محترفاً للنشاط الإجرامى أو عائداً فى سلوكه الخارج. فهو نمط مختلف، ينظر إليه المجتمع نظره مختلفة عن المجرم العادى(١).

سادساً: الأضرار:

تقع الجرائم المعلوماتية فى نطاق تقنية مقدمة يتزايد يوماً بعد يوم استخدامها فى إدارة المعاملات الاقتصادية والمالية – الوطنية والدولية – والاعتماد عليها فى تسيير معظم شئون الحياة اليومية للأفراد والشئون العامة لأكثر الحكومات بما فى ذلك الأمن والدفاع. ومن شأن ذلك أن يضفى أبعاداً غير مسبوقة على الخسائر والأضرار التى تنجم عن هذه الجرائم.

ولا أدل على ذلك من أن الخسائر المادية الناجمة عن هذه الجرائم تبلغ – وفقاً لتقديرات المركز الوطنى لجرائم الحاسب فى الولايات المتحدة الأمريكية (N.C.C.C.D) فى نهاية القرن الماضى حوالى ٥٠٠ مليون دولار فى السنة، بينما تقدرها مصادر أخرى بما يتراوح بين ٣:٥ بليون دولار فى السنة(٢).

---

(١) يراجع فى هذا الشأن:

- Jack Bologna, Corporate Fraud. The Basic of Prevention and Detection, Butter Worth, 1984, p. 11.

(2) Wasik (Martin): Crime and the Computers. 1991. p. 19.

سابعاً: صعوبة الاكتشاف والإثبات:

الجرائم المعلوماتية لا عنف فيها(*). ولا سفك للدماء، ولا آثار لاقتحام لسرقة أموال، وإنما هى أرقام وبيانات تتغير أو تمحى من السجلات المخزنة فى ذاكرة الحاسبات، ولأنها لا تترك أثراً خارجياً مرئياً. تكون صعبة الاكتشاف(**). ومما يزيد من هذه الصعوبة ارتكابها عادة فى خفاء، وعدم وجود أثر كتابى لما يجرى خلال تنفيذها من عمليات، حيث يتم بالنبضات الاليكترونية نقل المعلومات، وإمكانية ارتكابها عبر الدول والقارات باستخدام شبكات الاتصال ودون تحمل عناء الانتقال، والأحجام فى مجتمع الأعمال عن الإبلاغ عنها تجنباً للإساءة إلى السمعة وهز الثقة فى كفاءة المنظمات (المجنى عليها)، فضلاً عن إمكانية تدمير المعلومات التى يمكن أن تستخدم كدليل فى الإثبات فى مدة تقل عن الثانية.

وقد ذهب رأى إلى صعوبة قبول الرأى المتقدم على أطلاقه مهللاً ذلك بما يلى[1]:

---

(*) وهى ليست بلا عنف من وجهة نظر مكتب التحقيقات الفيدرالى الأمريكى (F.B.J.) الذى يرى «جرائم الحاسب» Computer Crimes كجرائم عنف As Voilent crimes استناداً إلى اكتشاف مكتب المحققين به أن دوافع المتلصصين والدخلاء على نظم الحاسبات تماثل دوافع مشعلى الحرائق ومفجرى القنابل والمفرقعات، يراجع:
د/ هشام رستم – المرجع السابق – هامش ٢ – ص ٤١.

(**) البيانات التى يتم تغييرها أو محوها من السجلات المخزنة، تتم ولا يستطيع القارئ العادى أن يعرف البيانات التى كانت مثبته قبل تغييرها أو محوها، فيكون من العسير اكتشافها.
أنظر عرضاً لمصادر صعوبة اكتشاف الجرائم المعلوماتية وإثباتها وبعض سمات مرتكبيها ودوافعهم لدى:
ج.ن. ميتاريهان – الدعاوى ضد مرتكبى الجرائم المرتبطة بالحاسب الإلكترونى – مقالة بالمجلة الدولية للشرطة الجنائية (الطبعة العربية) – العدد ٣٦٩ – يوليو ١٩٨٣ – ص ص ١٩٠، ١٩١.

(١) د/ نائلة عادل محمد فريد فورة – جرائم الحاسب الاقتصادية – مرجع سابق – ص ٤٤.

فمن ناحية لا يقتصر أثر جرائم المعلوماتية على تغيير أو محو الأرقام والبيانات من الملفات المخزنة في ذاكرة الحاسبات، بل أنه حتى فى هذه الحالات فمجرد تغيير أو محو هذه البيانات يعد أثراً على ارتكاب الفعل. فصعوبة اكتشافها وإثباتها يرجع إلى عدة أسباب من بينها وسيلة تنفيذها،والتى تتسم فى أغلب الحالات بالطابع التقنى الذى يضفى عليها الكثير من التعقيد.

ومن ناحية أخرى الإحجام عن الإبلاغ، وإمكانية تدمير المعلومات تعد من عناصر هذه الصعوبة.

ونحن لا نتفق مع الرأى الأخير فيما ذهب إليه، وحجتنا فى ذلك:

- ان الرأى الذى ذهب إلى أن الجريمة المعلوماتية لا تترك أثراً خارجياً مرئياً تكون صعبة الاكتشاف. هو بذلك يذكر خاصية يمكن أن تتمتع بها الجريمة المعلوماتية تميزها عن غيرها من الجرائم التقليدية.
- ثم زاد فى توضيح الأمر بتعديل زيادة الصعوبة على أمور أخرى متتابعة. تتكامل فى النهاية لتوضح علة صعوبة اكتشاف الجريمة المعلوماتية.

**ثامناً: الصيغة الدولية للجريمة المعلوماتية:**

يمكن القول - وبحق - أن من أهم الخصائص التى تميز الجريمة المعلوماتية هى تخطيها للحدود الجغرافية، ومن ثم اكتسابها طبيعة دولية، أو كما ذهب البعض أنها جريمة ذات طبيعة متعدية الحدود.

فمع ظهور شبكات المعلومات لم يعد هناك حدود مرئية أو ملموسة تقف أمام نقل المعلومات عبر الدول المختلفة. فالقدرة التى تتمتع بها الحاسبات الآلية فى نقل وتبادل كميات كبيرة من المعلومات بين أنظمة يفصل بينها آلاف الأميال، قد أدت إلى نتيجة مؤداها أن أماكن متعددة - منشآت وهيئات وشركات - فى دول مختلفة قد تتأثر بالجريمة المعلوماتية المرتكبة فى آن واحد. كما أن السرعة الهائلة فى تنفيذ الجريمة المعلوماتية

وحجم المعلومات ميزت الجريمة المعلوماتية عن نظريتها التقليدية بصورة كبيرة(١).

وتظهر هذه المشكلة بصفة خاصة فى مجال البنوك، حيث أدى التوسع الكبير فى إجراء المعاملات البنكية عبر شبكات المعلومات الدولية إلى إعطاء بعد دولى لجرائم الاحتيال المعلوماتى بصفة خاصة. حيث أدى ربط وسائل الأتصالات بالحاسبات الآلية إلى مضاعفة المعاملات المالية الدولية التى تتم بوسائل إلكترونية، وبصفة خاصة من خلال التحويل الإلكترونى للأموال "Electronic Funds Transfer"، والتبادل الإلكترونى للمعلومات Electronic Data Interchange".

ولا يقتصر الأمر على المعاملات المالية فقط، بل إن الطبيعة الدولية للجريمة المعلوماتية تظهر فى أنماط أخرى من السلوك:

- فقد يوجد الجانى فى دولة ويتمكن من الدخول إلى ذاكرة حاسب آلى موجود فى دولة أخرى، للقيام بعمل اجرامى فى نطاق المعلوماتية يضر بشخص آخر موجود فى دولة ثالثاً. (مثل جرائم النصب المعلوماتى).
- فيما يتعلق بالإتلاف المعلوماتى، فإعداد أحد البرامج الخبيثة (الفيروسات) يمكن أن يتم فى دولة ما، ثم يتم نسخ هذا البرنامج مرات عديدة ويرسل إلى دول متفرقة من العالم(*).

---

(١) د/ نائلة عادل قورة – المرجع السابق – ص ٤٧.

(*) من القضايا الهامة ذات البعد الدولى لجرائم المعلوماتية. قضية نقص المناعة المكتسبة (الإيدز). وتتلخص وقائعها أنه عام ١٩٨٩ قام أحد الأشخاص، بتوزيع عدد كبير من النسخ الخاصة بأحد البرامج الذى يهدف فى ظاهرة إلى اعطاء بعض النصائح الخاصة بمرض نقص المناعة المكتسبة. إلا أن هذا البرنامج فى حقيقته كان يحتوى على فيروس (من أمثلة حصان طراودة)، وكان يترتب على مجرد تشغيله تعطيل جهاز الحاسب الآلى عن العمل، ثم تظهر بعد ذلك على الشاشة عبارة يقوم الفاعل من خلالها بطلب مبلغ من المال يرسل على عنوان بدولة بنما حتى يتمكن المجنى عليه من الحصول على مضاد للفيروس. وفى الثالث من عام ١٩٩٠ تم إلقاء القبض على المتهم ويدعى/ جوزيف بوب فى ولاية أوهايو U.S.A، وتقدمت بريطانيا بطلب

=/=

## المطلب الثالث

## سمات المجرم المعلوماتي

لم يكن لارتباط الجريمة المعلوماتية بالحاسب الآلي أثره على تمييز الجريمة المعلوماتية عن غيرها من الجرائم التقليدية لحسب، وإنما كان له أثره أيضاً على تمييز المجرم المعلوماتى عن غيره من المجرمين الذين جنحوا إلى السلوك الإجرامي النمطي.

ولقد اختلف الباحثون فى تحديد السمات المميزة للمجرم المعلوماتى، كما اختلفوا أيضا فى مدى انطباق وصف جرائم ذوى الياقات البيضاء على مجرمى المعلوماتية. كما ثبت عدم جدوى النظرة التقليدية للمجرم المعلوماتى التى سادت فى كتابات الباحثين لفترة من الزمن. فمجرمو المعلوماتية ليسوا دائماً مجموعة من النوابغ الذين لا يمكن التنبؤ بسلوكهم أو معرفتهم، فإذا كان هذا النمط موجود بالفعل إلا أن النمط السائد هو المجرم الذى تربطه بالمجنى عليه صلة ما والتى غالباً ما تكون صلة وظيفية(1)، ولهذا يمكن القول بأن ثمة حقيقة واحدة اتفق

--- لتسليم المتهم لمحاكمته أمام القضاء الانجليزى، حيث أن ارسال هذا البرنامج تم من داخل المملكة المتحدة. وبالفعل وافق القضاء الأمريكى على تسليم المتهم، وتم توجيه إحدى عشر تهمة ابتزاز بحقه وقعت معظمها فى دول مختلفة، إلا أن اجراءات محاكمة المتهم لم يستمر بسبب حالته العقلية. وأيا ما كان الأمر فإن هذه القضية تظهر أهميتها من ناحيتين:

**الأولى:** أنها المرة الأولى التى يتم فيها تسليم متهم فى جريمة معلوماتية.

**الثانية:** أنها المرة الأولى أيضاً التى يقدم فيها شخص للمحاكمة بتهمة إعداد برنامج خبيث (فيروس).

أنظر:

- Clough (Bryan) & Mango (Paul), Approaching Zero: Data Crime and the criminal underworld, 1992, pp. 136-146.

مشار إليه لدى: د/ نائلة عادل قورة – المرجع السابق – ص ٤٨.

(1) Cornwall (Hugo), Datatheft, Computer Fraud, Industrial espionage and Information Crime, 1987, p. 134.

عليها الباحثون، وهى أن العدد الأكبر من جرائم المعلوماتية قد تم ارتكابها عن طريق أشخاص تربطهم علاقة بالمجنى عليهم سواء كانت علاقة وظيفية أو أى علاقة أخرى مباشرة.

ومع ذلك يمكن أن نستخلص مجموعة من السمات التى يتميز بها المجرم المعلوماتى، والتى يساعد التعرف عليها مواجهة هذا النمط الجديد من المجرمين. ويعد الأستاذ Parker واحداً من أهم الباحثين الذين عنوا بالجريمة المعلوماتية بصفة عامة وبالمجرم المعلوماتى بصفة خاصة، ويرى الأستاذ/ باركر بداية أن المجرم المعلوماتى وإن كان يتميز ببعض المسات الخاصة إلا أنه لا يخرج فى النهاية عن كونه مرتكباً لفعل إجرامى يتطلب توقيع العقاب عليه. فكل ما فى الأمر أنه ينتمى إلى طائفة خاصة من المجرمين تقترب فى سماتها من جرائم ذوى الياقات البيضاء، وإن كانت - فى رأيه - لا تتطابق معها. فالمجرم المعلوماتى، من ناحية، ينتمى فى أكثر الحالات إلى وسط اجتماعى متميز، كما أنه على درجة من العلم والمعرفة وهو ما يميز بشكل عام ذوى الياقات البيضاء، وإن كان ليس من الضرورى أن ينتمى المجرم المعلوماتى إلى مهنة يرتكب من خلالها الفعل الإجرامى كما هو الحال فى جرائم ذوى الياقات البيضاء، كما يتفق مجرم المعلوماتية مع ذوى الياقات البيضاء فى أن الفاعل فى الحالتين يبرر جريمته، بل إنه لا ينظر إلى سكوكه باعتباره جريمة أو فعل يتنافى مع الأخلاق[1].

---

(1) suthreland (Edwin H.), "White-Collar criminality", in Geis (Gilbert) (ed.), White Collar Criminal: The Offender in Business and the Professions, 1968.

## الفرع الأول

## الخصائص المميزة للمجرم المعلوماتي

يتميز المجرم المعلوماتى - كذلك - بمجموعة من الخصائص التى تميزه بصفة عامة عن غيره من المجرمين، ويرمز إليها الأستاذ (PARKER) بكلمة Skram وهى تعنى المهارة Skills المعرفة Knowledge، الوسيلة Resources ، السلطة Authority ، وأخيراً الباعث Motives (١).

- **المهارة:**

تعد المهارة المتطلبة لتنفيذ النشاط الإجرامى أبرز خصائص المجرم المعلوماتى. فتنفيذ الجريمة المعلوماتية بصفة عامة يتطلب قدراً من المهارة يتمتع بها الفاعل، والتى قد يكتسبها عن طريق الدراسة المتخصصة فى هذا المجال، أو عن طريق الخبرة المكتسبة فى مجال تكنولوجيا المعلوماتى، أو بمجرد التفاعل الاجتماعى مع الآخرين. إلا أن ذلك لا يعنى ضرورة أن يكون المجرم المعلوماتى على قدر كبير من العلم فى هذا المجال، أو أن تكون لديه خبرة كبيرة فيه، بل إن الواقع العملى قد أثبت أن جانب من أنجح مجرمى المعلوماتية، لم يتلقوا المهارة اللازمة لإرتكاب الجريمة عن طريق التعليم أو الخبرة المكتسبة من العمل فى هذا المجال (٢).

- **المعرفة:**

تعنى المعرفة التعرف على كافة الظروف التى تحيط بالجريمة المراد تنفيذها، وإمكانيات نجاحها واحتمالات فشلها، فالجناة عادة يمهدون لارتكاب جرائهم بالتعرف على كافة الظروف المحيطة، لتجنب الأمور غير المتوقعة التى من شأنها ضبط أفعالهم والكشف عنهم. وتميز المعرفة بمفهومها السابق مجرمى

---

(1) Parker (Donn B.), Op. cit., pp. 136 - 138.

(٢) د/ نائلة عادل قورة - المرجع السابق - ص ٥٢.

المعلوماتية، حيث يستطيع المجرم المعلوماتى أن يكون تصوراً كاملاً لجريمته، ويرجع ذلك إلى أن المسرح الذى تمارس فيه الجريمة المعلوماتية هو نظام الحاسب الآلى، فالفاعل يستطيع أن يطبق جريمته على أنظمة مماثلة لتلك التى يستهدفها وذلك قبل تنفيذ جريمته.

- **الوسيلة:**

الوسيلة يراد بها الإمكانيات التى يتزود بها الفاعل لإتمام جريمته. وفيما يتعلق بالمجرم المعلوماتى فإن الوسائل المتطلبة للتلاعب بأنظمة الحاسب الآلية هى فى أغلب الحالات تتميز نسبياً بالبساطة وبسهولة الحصول عليها. فالمجرم المعلوماتى يتميز بقدرته فى الحصول على ما يحتاج إليه أو ابتكار الأساليب التى تقلل من الوسائل اللازمة لإتمام النشاط الإجرامى. والحقيقة أنه كلما كان نظام الحاسب الآلى الذى يحتوى على المعلومات المستهدفة غير مألوف، كانت الوسائل المتطلبة أكثر صعوبة فى الحصول عليها، لاقتصارها على عدد قليل من الأفراد هم عادة القائمون على تشغيل النظام، وذلك على عكس الأنظمة الشائعة الاستعمال (برامج مايكروسوفت على سبيل المثال).

- **السلطة:**

يقصد بالسلطة فيقصد بها الحقوق أو المزايا التى يتمتع بها المجرم المعلوماتى والتى تمكنه من ارتكاب جريمته. فكثير من مجرمى المعلوماتية لديهم سلطة مباشرة أو غير مباشرة فى مواجهة المعلومات محل الجريمة. وقد تتمثل هذه السلطة فى الشفرة الخاصة بالدخول إلى النظام الذى يحتوى على المعلومات، والتى تعطى الفاعل مزايا متعددة كفتح المفات وقراءتها وكتابتها ومحو أو تعدل المعلومات التى تحتوى عليها. وقد تتمثل هذه السلطة فى الحق فى استعمال الحاسب الآلى، أو إجراء بعض التعاملات، أو مجرد الدخول إلى الأماكن التى تحتوى على أنظمة الحاسبات الآلية. وقد تكون السلطة التى يتمتع بها الجانى غير شرعية، كما فى حالة استخدام شفرة الدخول الخاصة بشخص آخر.

• الباعث(*):

وأخيراً يأتى الباعث وراء ارتكاب الجريمة، ولا يختلف باعث الجانى على ارتكاب الجريمة المعلوماتية فى كثير من الأحيان عن الباعث لارتكاب غيرها من الجرائم الأخرى، فالرغبة فى تحقيق الربح المادى بطريق غير مشروع يظل الباعث الأول وراء ارتكاب الجريمة المعلوماتية(1). ثم يأتى بعد ذلك مجرد الرغبة فى قهر نظام الحاسب وتخطى حواجز الحماية المضروبة حوله. وأخيراً الانتقام من رب العمل أو أحد الزملاء(**).

---

(*) الدافع أو الباعث أو الغرض أو الغاية، تعبيرات لكل منها دلالته الاصطلاحية فى القانون الجنائى، تتصل بما يعرف بالقصد الخاص فى الجريمة، وهى مسألة تثير جدلاً فقهياً وقضائياً واسعاً، ذلك أن «القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجنائى». (د/ محمود نجيب حسنى - شرح قانون العقوبات (القسم العام) - دار النهضة العربية - سنة ١٩٨٩ - ص ١٠٥٢).

وأن الباعث «لا أثر له فى وجود القصد الجنائى». (د/ أحمد فتحى سرور - الوسيط فى قانون العقوبات (القسم العام) - دار النهضة العربية - ط ٥ - سنة ١٩٩١ - ص ٣٢٧).

وإذا كان الإستخدام العادى للتعبيرات المشار إليها يجرى على أساس ترادفها فى الغالب، فإنها من حيث الدلالة تتمايز، وينتج عن تمايزها أثار قانونية على درجة كبيرة من الأهمية.

فالباعث هو: «العامل المحرك للارادة الذى يوجه السلوك الإجرامى، كالمحبة والشفقة والبغضاء والانتقام». (د/ كامل السعيد -

وهو اذن قوة نفسية تدفع الإدارة إلى الاتجاه نحو ارتكاب الجريمة، ابتغاء تحقيق غاية معينة.

(1) ويرى البعض أن أغلب مجرمى المعلوماتية ليست لديهم أطماع مادية بقدر ما يحاولون حل مشكلات مادية تواجههم لا يستطيعون حلها باللجوء إلى الجرائم الأخرى. أنظر:

- Parker (Donn), Op. cit., p. 142.

(**) والحقيقة أنه آياً ما كان الباعث وراء ارتكاب الجريمة المعلوماتية فإنه يوجد شعور دائماً لدى مرتكب الفعل بأن ما يقوم به لا يدخل فى عداد الجرائم، أو بقول آخر لا يمكن أن يتصف باللاأخلاقية، وخاصة فى الحالات التى يقف فيها السلوك عند حد قهر نظام الحاسب الآلى وتخطى الحماية المضروبة حوله، حيث يفرق مرتكبو هذه الجرائم بين الإضرار بالأشخاص الأمر الذى يعدونه غاية فى اللاأخلاقية وبين الإضرار بمؤسسة أو جهة فى استطاعتها اقتصادياً تحمل نتائج تلاعبهم وهو ما يطلق عليه أعراض روبن هود "The robin Hood Syn-drome". (د/ هشام رستم - مرجع سابق - ص ٣٨).

## الفرع الثاني

## تصنيف مجرمي المعلوماتية

يقسم مجرمي المعلوماتية "Cybercriminals" إلى مجموعة من الطوائف المختلفة، حيث أسفرت الدراسات المختلفة في هذا المجال عن وجود سبعة أنماط من مجرمي المعلوماتية(1). ولا يعني ذلك بطبيعة الحال أن كل مجرم يندرج تحت طائفة محددة دون غيرها بل يمكن أن يكون المجرم الواحد مزيجاً من أكثر من طائفة، وتتمثل هذه الطوائف فيما يأتي(*):

تضم الطائفة الأولى "Pranksters" الأشخاص الذين يرتكبون جرائم المعلوماتية بغرض التسلية والمزاح مع الآخرين بدون أن يكون في نيتهم إحداث أي ضرر بالمجني عليهم، ويندرج تحت هذه الطائفة بصفة خاصة صغار مجرمي المعلوماتية (الأحداث)(**).

---

(1) Parker (Donn B.). Op. cit./, pp. 144 - 146.

(*) ذهب رأي إلى أنه من أفضل التصنيفات لمجرمي التقنية، التصنيف الذي أورده David Icove, Karl Seger & william Vons Torch في مؤلفهم جرائم الكمبيوتر – عام ١٩٩٥ – حيث تم تقسيم مجرمي التقنية إلى ثلاثة طوائف: المخترقون (المتطفلون)، والمحترفون، والحاقدون. كما أن من بين التصنيفات الهامة التمييز بين صغار السن من مجرمي المعلوماتية وبين البالغين، الذين يتجهون للعمل معاً لتكوين المنظمات الإجرامية الخطرة.

- David Icove, Karl seger and william vonstorch: Computer Crime, a crime fighter's Handbook (95 Edition) available at htt:// www. Powells - Com/biblio? show: 1565920864.

مشار إليه لدى:

أيمن عبد الله فكري – جرائم نظم المعلومات – رسالة مقدمة للحصول على درجة الدكتوراه – كلية الحقوق – جامعة المنصورة – سنة ٢٠٠٥ – ص ٧٨.

(**) تعددت أوصاف هذه الطائفة في الدراسات الاستطلاعية والاحصائية، وشاع في نطاق الدراسات الإعلامية والتقنية وصفهم بمصطلح (المتلعثمين)، ويعني حسب وصف أحد المتخصصين: (الصغار المتحمسون للحاسب، بشعور من البهجة، دافعهم التحدي لكسر الرموز السرية لتركيبات الحاسب). وأطلق عليهم البعض (مجانين معدلات ومعدلات عكسية)، استناداً إلى كثرة استخدامهم لتقنية المعدل والمعدل العكسي (الموديم).

—/—

• المخترقون:

أما الطائفة الثانية "Hackers" فهى تضم الأشخاص الذين يستهدفوا من الدخول إلى أنظمة الحاسبات الآلية الغير مصرح لهم بالدخول إليها كسر الحواجز الأمنية الموضوعة لهذا الغرض، وذلك بهدف اكتساب الخبرة أو بدافع الفضول، أو لمجرد إثبات القدرة على اختراق هذه الأنظمة.

* المخترق المؤذي (الخبيث):

وتتضمن الطاقة الثالثة "Malicious hackers" أشخاصاً هدفهم إلحاق خسائر بالمجني عليهم، دون أن يكون الحصول على مكاسب مادية من ضمن هذه الأهداف، ويندرج تحت هذه الطائفة الكثير من مخترعى فيروسات الحاسبات الآلية وموزعيها.

• حل المشاكل الشخصية:

أما الطائفة الرابعة "Personal Problem Solvers" فهم الطائفة الأكثر شيوعاً بين مجرمى المعلوماتية، فهم يقومون بارتكاب جرائم المعلوماتية بحيث يترتب عليها فى كثير من الآحيان خسائر كبيرة تلحق بالمجنى عليه. ولا يكون الباعث على ارتكاب الجريمة تحقيق ربح مادى، بقدر ما هو الرغبة فى إيجاد حلول لمشكلات مادية تواجه الجانى، ولا يستطيع حلها بالوسائل الأخرى، بما فيها اللجوء إلى الجريمة التقليدية. كما أنهم يتمتعون بقدر معقول من الخبرة فى مجال الحاسبات الآلية وذلك بحكم عملهم. ويبرر المنتمون إلى هذه الطائفة أفعالهم دائماً، بحيث لا يجدون غضاضة فى ارتكاب الفعل بحجة أن المجنى

---

-- وقد ظهرت دراسات ومؤلفات بحثيه تدافع عن هذه الفئة، لتخرجهم من دائرة الاجرام إلى دائرة العبث، وأحياناً البطولة.

- Tom forester: Essential Problems to High - Tech Society first Mit Pres- edition, Cambridge, Massachusetts, 1989, p. 409.

عليه – والذى غالباً ما يكون مؤسسة مالية ينتمى إليها الفاعل – يستطيع أن يتحمل الخسائر الناجمة عن أفعالهم.

وتتضمن الطائفة الخامسة "Career Criminals": مجرمى المعلوماتية الذين يبتغون من وراء نشاطهم الإجرامى تحقيق الربح المادى بطريقة غير مشروعة. ويعمل المنتمون إلى هذه الطائفة فى أغلب الأحوال بطريقة منظمة بحيث ينطبق على أفعالهم وصف الجريمة المنظمة، أو على الأقل يشترك فى تنفيذ النشاط الإجرامى أكثر من فاعل، ويقترب المجرم المعلوماتى المنتمى إلى هذه الطائفة فى سماته من المجرم التقليدى(*).

أما الطائفة السادسة "extreme Advocates" فتدخل فى عدادها الجماعات الإهابية أو المتطرفة، والتى تتكون بدورها من مجموعة من الأشخاص لديهم معتقدات وأفكار اجتماعية أو سياسية أو دينية ويرغبون فى فرض هذه المعتقدات باللجوء أحياناً إلى النشاط الإجرامى، ويتركز نشاطهم بصفة عامة فى استخدام العنف ضد الأشخاص والممتلكات من أجل لفت الأنظار إلى ما يدعون إليه. ولقد بدأ اهتمام الجماعات الإهابية، وخاصة التى تتمتع من بينها بدرجة عالية من التنظيم، يتجه إلى نوع جديد من النشاط الإجرامى ألا وهو الجريمة المعلوماتية. فاعتماد المؤسسات المختلفة داخل الدول على أنظمة الحاسبات الآلية فى إنجاز أعمالها والأهمية القصوى للمعلومات التى تحتويها فى أغلب الأحوال، قد جعل من هذه الأنظمة هدفاً جذاباً لتلك الجماعات(**).

---

(*) ولا شك فى أن جرائم الحاسبات الآلية بدأت تجذب بشكل كبير اهتمام الجماعات الإجرامية المنظمة نظراً لإرتفاع قيمة ما تدره من أرباح مادية مع صعوبة الكشف عنها وإثباتها بالمقارنة بالجرائم التقليدية، إلا أن نسبة هذا النمط مع ذلك مازالت منخفضة بالمقارنة بغيره من الأنماط الأخرى (١,٥ ٪) ويرجع ذلك بصفة أساسية لما تتطلبه هذه الجريمة من توافر درجة من العلم بتقنية الحاسبات وهو ما لا يتوافر لدى الكثيرين من هذه الطائفة.

(**) ولا تزال الأمثلة فى هذا المجال قليلة وإن كان من المتوقع أن تزداد مستقبلاً، ومن الأمثلة الشهيرة فى هذا الخصوص قيام إحدى الجماعات الإرهابية المعروفة فى أوروبا باسم "The Red Brigades: بتدمير ما يزيد عن ٦٠ مركزاً للحاسبات الآلية خلال الثمانينيات لتلفت الأنظار إلى أفكارها ومعتقداها.

• **مجرمي الأهمال:**

وأخيرا تأتى الطائفة السابعة "The Criminally Negligent" والتى تضم واحدة من أهم المشكلات التى تتصل بإساءة استخدام الحاسبات الآلية ألا وهى الإهمال. ولا شك فى أن الإهمال فى مجال الحاسبات ا لآلية يمكن أن يترتب عليه فى كثير من الأحيان نتائج خطيرة قد تصل إلى حد إزهاق الروح.

ففى نيوزيلندا، (على سبيل المثال) قام اثنان من مبرمجى الحاسبات الآلية بتغيير فى أحد البرامج، التى تحدد خط سير إحدى الطائرات ولم يتمكنوا من إبلاغ قائد الطائرة بهذه التغييرت، مما ترتب عليه تحطم الطائرة لاصطدامها بأحد الجبال وقتل ٦٠ راكباً كانوا على متنها، ولقد تمت محاكمة المتهمين بتهمة القتل الخطأ.

والحقيقة أنه أياً ما كانت درجة الدقة فى رسم حدود كل طائفة من الطوائف ينتمى إليها مجرموا المعلوماتية فإننا نرى أن البواعث الرئيسية على ارتكاب الجريمة المعلوماتية والتى تحدد الطائفة التى ينتمى إليها المجرم المعلوماتى لا تخرج عن ثلاثة بواعث تحرك المجرم المعلوماتى[١]: -

- الباعث الأول فتشترك فيه الجريمة المعلوماتية مع غيرها من جرائم الاعتداء على الأموال وهو تحقيق الربح المادى.

فى حين يميز الباعث الثانى الجريمة المعلوماتية عن غيرها، ويتمثل فى الرغبة فى الدخول إلى أنظمة الحاسبات الآلية والمعلوماتية التى تحتويها، لا لغرض سوى التسلية أو إثبات الخبرة التقنية التى يتمتع بها الفاعل، أو غير ذلك

---

(١) د/ نائلة قورة – المرجع السابق – ص ٥٩.
وأيضاً انظر فى شرح لهذه البواعث:
- Rose (Philipe): La Criminalité Informatique tique à L'Horizon, 2005, p. 69.

من الأغراض التى لا يكون السعى إلى تحقيق ربح مادى أو الإضرار بهذه الأنظمة من بينها.

وأخيراً يأتى الباعث الثالث والذى يتمثل فى الرغبة فى الإضرار بهذه الأنظمة، سواء كانت هذه الرغبة بدافع الانتقام من المؤسسات التى تنتمى إليها هذه الأنظمة أو لمجرد الإضرار بها بدافع المنافسة أو غير ذلك، وينتمى إلى هذه الطائفة مستخدمو فيروسات الحاسبات الآلية.

وختاماً نضيف أن الدراسات القليلة للجوانب السيكولوجية لمجرمى المعلوماتية، أظهرت شيوع عدم الشعور بلا مشروعية الطبيعة الإجرامية، وبلا مشروعية الأفعال التى يقترفونها، كذلك الشعور بعدم استحقاقهم للعقاب عن هذه الأفعال، فحدود الخير والشر متداخلة لدى هذه الفئة، وتغيب بداخلهم مشاعر الإحساس بالذنب. لقد أنشأ الاستخدام المتزايد للحاسبات الآلية لدى هذه الفئة مناخاً نفسياً موائماً لتصور استبعاد فكرة الخير والشر، وساعد على ذلك عدم وجود احتكاك مباشر بين الأشخاص والتباعد بين الفاعل والمجنى عليه.

## المبحث الثاني

## الجريمة المعلوماتية والقواعد العامة في القانون

### المطلب الأول

### الشروع في الجريمة المعلوماتية

يراد بالشروع La Tentative في الجريمة ذلك السلوك الذى يهدف به صاحبه إلى ارتكاب جريمة معينة، كانت لتقع بالفعل لولا تدخل عامل خارج عن إرادة الفاعل حال فى اللحظة الأخيرة دون وقوعها(١).

فالشارع فى الجريمة هو فى الحقيقة مجرم بكل معنى هذه الكلمة، لأن وقوع الجريمة منه كان قد صار قاب قوسين أو أدنى، وإذا كانت الجريمة قد تخلفت فى صورتها التامة، فإنما يرجع هذا إلى تدخل عامل لا شأن لإرادته فيه هو الذى حال دون تحققها(*).

ويصبح العقاب محل دون شك حين يحسم الإنسان النية على ارتكاب الجريمة ويقدم بالفعل على تنفيذها، بحيث لا يتبقى ثمة حائل دون وقوعها، لولا عامل تدخل من الوسط المحيط فمنع تحققها فى أخر لحظة استقلالا عن إرادة

---

(١) د/ رمسيس بهنام – النظرية العامة للقانون الجنائى – منشأة المعارف – الاسكندرية – طبعة سنة ١٩٩٥ – ص ٥٨٣.

(*) وعلى هدى ما تقدم، لا يمكن أن ينعت بوصف المجرم (المعلوماتى) إنسان لم يصل به السلوك إلى تلك المرحلة، وإنما تساوره نفسه بأن يرتكب الجريمة – من جرائم الحاسب الآلى – وربما يعد العدة لها ويحضر وسائل تنفيذها، وذلك لأن النفس أمارة بالسوء، وتكاد لا تخلو نفس إنسان من تفكير فى إلحاق أذى بغيره. فمهما كانت الأفكار السيئة تساور النفس، ومهما اتخذ التعبير عنها مظهراً خارجياً كإعداد عدة التنفيذ، يحتمل دائماً أن يتوب صاحب تلك الأفكار إلى رشده وأن يعدل عن الإصرار على تنفيذ ما يحتمل فى صدره. (المرجع السابق – ص ٥٨٤).

الفاعل ورغما عنها(*). ذلك مـا عنتـه المادة (٤٥) من قـانون العـقـوبات حين نصت على أن:

«الشروع هو البدء فى تنفيذ فعل بقصد إرتكاب جناية أو جنحة إذا أوقف أو خاب أثره لأسباب لا دخل لإرادة الفاعل فيها.

ولا يعتبر شروعاً فى الجناية أو الجنحة مجرد العزم على ارتكابها ولا الأعمال التحضيرية».

## الفرع الأول

## أركان الشروع في الجريمة المعلوماتية

يستفاد من التعريف بالشروع الوارد فى المادة ٤٥ من قانون العقوبات، أنه يقوم على أركان ثلاثة هى:

- البدء فى تنفيذ الجريمة.
- بقصد ارتكابها.
- يوقف أو يخيب أثره لسبب لا دخل لإرادة الفاعل فيه.

**( أ ) البدء في التنفيذ:**

إن فيصل التفرقة بين ما هو محض تحضير للجريمة غير معاقب عليه، وبين ما هو بدء فى تنفيذها يعاقب عليه القانون، ليس من اليسير تحديده حيث آثار جدلاً فقهياً كبيراً - يخرج عن نطاق دراستنا - سوف نعرض لأبرز الاراء بشأنه بما يثرى نطاق البحث لدينا.

---

(*) وفى ضوء العقاب على الشروع، ذهب الأستاذ الدكتور/ رمسيس بهنام إلى أن محض التصميم على الجريمة أو الأعمال التحضرية لها أمر لا عقاب عليه، على أن التصميم قد يعاقب عليه كجريمة خاصة لا بوصفه شروعاً فى الجريمة المصمم عليها، كما هو الحال فى الأتفاق على ارتكاب جناية أو جنحة (م ٤٨ ع)، والإتفاق على ارتكاب جرائم مخلة بأمن الدولة مما نصت عليه المادة (٩٦ ع)، والتحريض على ارتكاب هذه الجرائم (م ٩٥ ع)، وقد يعاقب العمل التحضيرى لا بوصفه شروعاً فى الجريمة الجارى التحضير لها، وإنما بوصفه جريمة خاصة كما فى العقاب على صنع المفاتيح وتقليدها مع توقع أستعمالها فى ارتكاب جريمة (م ٣٢٤ ع). (المرجع السابق - هامش ٥٨٤).

- **فهناك المذهب المادي:** طبقاً لذلك المذهب يلزم أن يكون الفاعل قد حقق عملاً بداية الركن المادى للجريمة كما وصفه نموذجها، وإلا فلا يعتبر سلوكه شروعاً فى الجريمة ولا ينال على السلوك عقاباً(١). فلا يعتبر الشخص شارعاً فى السرقة إذا لم يكن قد وضع بعد يده على المال الذى يريد أن يختلسه.

وقد أخذ على هذا المذهب أنه يترك بدون عقاب جناه هم أهل للعقاب، بسبب ما يرد منهم من سلوك يقطع بإنحسام نيتهم على الجريمة، وإن كان لم يبلغ توغله فى طريقها الحد المتقدم(٢).

وقد حاول أنصار المذهب المادى علاج هذا القصور الذى يؤدى إليه العمل بمذهبهم(*)، بمزيد أضيف إلى النظرية إكمالاً لها، مؤداه أنه يكفى لاعتبار الإنسان شارعاً، أن يكون قد تحقق بسلوكه ما يعتبر ظرفاً مشدداً لعقوبة الجريمة المشروع فى ارتكابها، ولو لم يكن قد حقق بعد سلوكه بداية النموذج الذى وصفت به الجريمة فى نص القانون.

- **المذهب الشخصي:** يذهب أنصار هذا المذهب - وعلى رأسهم الأستاذ (Garraud)(٣) - إلى القول بأن الشروع هو سلوك يؤدى حالاً ومباشرة إلى الركن المادى للجريمة، كما وصفها نموذجها فى القانون، ولو لم يكن السلوك قد حقق بالفعل بداية هذا الركن.

وبناء على ذلك لا يلزم لاعتبار شخص ما شارعاً فى السرقة أن يكون قد حاز بالفعل المال المنقول المقصود بالسرقة، وإنما يكفى أن يكون قد بلغ فى السلوك حداً يؤدى حالاً ومباشرة إلى هذه الحيازة.

(1) Villey: "Précis d'un cours de droit criminel", 1906, p. 86.

(2) Donnedieu de Vabres: "Traité de droit criminel et de législation Pénale Comparée", Pdris, 1947, p. 134.

(*) لم يوفق المذهب المادى مع هذا التعديل فى القضاء على ما يوجد به من قصور، ذلك لأن الظروف المشددة لكل جريمة ليست متفقة من حيث جواز اعتبار أى منها لو حدث بمثابة شروع فى ارتكاب الجريمة. (د/ رمسيس بهنام - المرجع السابق - ص ٥٨٦).

(3) Garraud: "Traité théorique et Pratique de Droit pénal", 1924 - 1935 t. Ipar, 232, p. 494.

وقد أنتقد الاستاذ (Roux) صيغة المذهب الشخصى من ناحية أن الفعل قد لا يؤدى فى الحال إلى الركن المادى للجريمة وإنما يستغرق فى سبيل بلوغ هذا الركن أياماً، كالحفر تحت الأرض توصلاً إلى خزائن بنك لسرقة ما بها من أموال. ومن ثم آثر الاكتفاء في تعريف الشروع بأنه: «العمل المؤدى مباشرة إلى ارتكاب الجريمة»(١).

- ويشار إلى أن قضاء محكمة النقض الفرنسية مستقر على الأخذ بالمذهب الشخصى، وعلى ترديد صياغته فى التعريف بالشروع(٢).

- الوضع في مصر: استقر قضاء محكمة النقض المصرية على الأخذ بالمذهب الشخصى(*)، كما أن آراء الفقة لا تخرج فى مؤداها عنه فى التعريف بالشروع(٣).

---

(١) تعليق Roux على حكم محكمة النقض الفرنسية فى ٣ يناير ١٩١٣ - S. 1913. I. 281

(٢) حكم بأنه يعتبر شروعاً فى السرقة التربص للمجنى عليه فى انتظار ان يمر للسطو عليه.

- Crim. 19 nov. 1943. Gaz, Pal. 1943 - 2 - 265.

أو الدخول فى الأماكن المراد ارتكاب السرقة فيها.

- Crim. 9 mai, 1956, Bull Crim, no. 362.

وأنه يعتبر شروعاً فى النصب ادعاء شخص وقوع حادث خيالى بغية الحصول على مبلغ تأمين، ورفع دعوى قضائية للمطالبة بهذا المبلغ من شركة التأمين.

- Crim. 5 déc, 1961, D. H, 1962, J. 201.

وبأن الشروع هو تلك الأفعال التى تكون نتيجتها المباشرة والحالة تنفيذ الجريمة.

... des actes devant avoir Pour conséquence directe et immédiate de consommer le crime.

(*) بعد أحكام قليلة أخذت فى البداية بالمذهب المادى، استقرت أحكام المحكمة العليا على العمل بالمذهب الشخصى وترديد صياغته.

فمثلاً اعتبر مجرد طلب الفحشاء من إمرأة وجذبها من يدها وملابسها عملاً تحضيرياً، لا بدءاً فى تنفيذ جريمة موافقة أنثى بغير رضاها. (نقض ٣٠ مارس ١٩١٢ المجموعة الرسمية س ١٣ – رقم ٥٩ – ص ١١٨). لابدءاً فى تنفيذها. (نقض ٢٦ يونيو ١٩٢٢ – المحاماة – س ٤ رقم ١٠).

(٣) راجع فى الفقه: الاستاذ/ على بدوى – الأحكام العامة فى القانون الجنائى – القاهرة – سنة ١٩٣٨ – ص ٢٠٠ وما بعدها، د/ محمد مصطفى القللى – مقالة عن الشروع – مجلة القانون

-/-

وقد حكم بأنه لا يشترط لتحقيق الشروع أن يبدأ الفاعل بتنفيذ جزء من الأعمال المكونة للركن المادى للجريمة، بل يكفى لاعتبار أنه شرع فى ارتكاب جريمة أن يبدأ بتنفيذ فعل سابق مباشرة على تنفيذ الركن المادى لها ويؤدى إليه حتماً(١).

وقضت محكمة النقض في حكم لها: «أن الافعال التى قام بها الطاعنون دخلت فعلاً فى دور التنفيذ وأنها قطعت أول خطوة من الخطوات المؤدية حالاً ومباشرة إلى ارتكاب السرقة التى اتفقوا على ارتكابها بحيث أصبح عدولهم بعد ذلك باختيارهم عن مقارفة الجريمة المقصودة بالذات أمراً غير محتمل»(٢).

كما حكم بأنه من المقرر أنه لا يشترط لتحقق الشروع أن يبدأ الفاعل تنفيذ جزء من الأعمال المكونة للركن المادى للجريمة، بل يكفى لاعتبار الفعل شروعاً فى حكم المادة ٤٥ من قانون العقوبات، أن يبدأ الجانى فى تنفيذ فعل سابق على تنفيذ الركن المادى للجريمة، ومؤد إليه حالاً ومباشرة(٣). فيعتبر شروعاً فى السرقة معالجة الشخص الباب الداخلى للمنزل بأدوات احضرها لكسره إلى أن كسر بعض أجزائه(٤).

وحكم بأن تحضير الأدوات والسبائك اللازمة للتزييف واستعمالها بالفعل فى اعداد العملة الزائفة التى لم تصل إلى درجة من الإتقان تكفل لها الرواج فى

---

= والاقتصاد – سنة ١٩٣١ – ص ٣١٩ وما بعدها، محمود ابراهيم اسماعيل – شرح الأحكام العامة في قانون العقوبات – القاهرة – سنة ١٩٣٩ – ص ٢٣٤ وما بعدها.

(١) نقض ٢٩ أكتوبر ١٩٣٤ – مجموعة القواعد القانونية – جـ٣ – رقم ٢٨٢ – ص ٣٧٥.

(٢) نقض ٢٥ ديسمبر ١٩٥٦ مجموعة القواعد القانونية – س ٧ – رقم ٣٦٣ – ص ١٣٢٠.

ومفاد الواقعة: أن عامل مكلف بنقل المازوت من شركة شل إلى شركة الصباغة والتجهيز، حصل على ختم الشركة الأخيرة الدال على تسلمها لكميات المازوت الخاصة بأحد الأيام، مع أن هذه الكمية لم تكن وصلت بعد ومازالت فى صهريج شركة شل، متفقاً مع بعض موظفى الصباغة والتجهيز على بيع المازوت وأقتسام ثمنه معهم.

(٣) نقض ١١ مارس ١٩٦٣ – مجموعة القواعد – س ١٤ – رقم ٣٧ – ص ١٧٨.

(٤) نقض ٤ أكتوبر ١٩٦٦ – مجموعة القواعد – س ١٧ – عدد ٣ – ص ٩١١.

المعاملة، يعتبر فى نظر القانون من أعمال الشروع المعاقب عليه قانوناً، إذ أن المتهمين بهذا قد تعديا مرحلة التفكير والتحضير، وانتقلا إلى دور التنفيذ، بحيث لو تركا وشأنهما لتمت الجريمة فى أعقاب ذلك مباشرة(١).

وتطبيقاً لذلك فى نطاق صور الاعتداء على نظام بطاقات الأئتمان، والمتمثلة فى إساءة استعمال البطاقة رغم إلغاء المصدر لها، فقد يلغى البنك المصدر بطاقة العميل لأى سبب من الأسباب، مثل غلق الحساب، أو تغيير نظام التعامل، أو تغيير نوعية الخدمة التى تؤديها البطاقة، ومع ذلك تظل البطاقة مع العميل وقد يستخدمها بعد إلغائها. ففى حالة إغلاق الحساب بمعرفة العميل، فإن استخدام ا لبطاقة الملغاة - كما ذهب الفقه الفرنسى(٢) - يعد شروع فى سرقة ما لم يتحصل على مال، لأن العميل على علم بأن ليس له حساب لدى البنك ويستعمل البطاقة بقصد الحصول على مال.

ويضيف رأى أنه يجب التفرقة فى هذه الحالة بين ما إذا كان هذا الاستعمال على حساب العميل المغلق بالبنك، وما إذا كان على حساب شخص آخر، ففى الثانية لا شك أن ذلك يعد شروعاً فى نصب إذا ضبطت البطاقة أثناء الاستعمال وقبل الحصول على المبلغ، أما وقد سهلت له البطاقة الحصول على مبلغ من حساب الغير، فتلك جريمة نصب تامة واعتداء على حقوق الغير(٣).

وإذا كان تحديد الشروع المعاقب عليه تكتنفه الصعوبات حين يتوقف الفاعل

---

(١) نقض ١٧ مايو ١٩٦٠ - مجموعة القواعد - س ١١ رقم ٨٩ - ص ٤٦٣.
ويراجع فى ذات المعنى: نقض ١٠ مايو ١٩٦٥ - مج - س ١٦ - رقم ٨٨ - ص ٤٤١.
وقد حكم بأن جريمة الشروع فى تقليد الأوراق المالية، تتحقق بقيام الجانى بطبع هذه الأوراق بما استعمله من آلة طبع وبما استخدمه من أدوات ومواد أخرى، ولو كان هناك نقص أو عيوب فى التقليد. نقض ٢٨ يونيو ١٩٦٥ - مج - س ١٦ - رقم ١٢٣ - ص ٦٣٢.

(2) JEANDIDIER (Wilfrid): "droit Pénal Général", Montchrestien, Paris, 1988, N°. 16, p. 225.

(٣) د/ إيهاب فوزى السقا - الحماية الجنائية والأمنية لبطاقات الأئتمان - دار الجامعة الجديدة - الإسكندرية - سنة ٢٠٠٧ - ص ١٧٦.

عن المضى فى سلوكه إلى النهاية، لتدخل عامل خارج عن إرادته حال دون ذلك، فإنه لا صعوبة على العكس فى ذلك التحديد، وفى القطع بوجود الشروع حين يكون الفاعل قد أسترسل فى السلوك إلى نهايته واستنفد بدون عائق ما كان فى وسعه، غير أن الحدث الإجرامى الذى كان يبغى بالسلوك تحقيقه هو الذى نهض من العوامل ما حال دون وقوعه(١).

ففى الحالة الأولى، يكون دور العامل الحائل منع السلوك من الاكتمال على الوجه المنشود، وفى الحالة الثانية، يكون دوره منع الحدث من الوقوع رغم اكتمال السلوك الذى اتخذ فى سبيل بلوغه.

وفى الحالتين، لا تتحقق الجريمة على الصورة الكاملة المطابقة لنموذجها الموصوف فى القاعدة الجنائية، إذ لا يتوافر منها فى الحالة الأولى سوى جزء من السلوك اللازم لارتكابها، ولا يتحقق منها فى الحالة الثانية سوى السلوك بأكمله وإنما بدون الحدث الذى كان يتطلب النموذج نشوءه من هذا السلوك، من أجل ذلك يطلق على الشروع فى الحالتين أسم الجريمة الناقصة، وتسمى هذه الجريمة الناقص بالجريمة الموقوفة فى الحالة الأولى، وبالجريمة الخائبة فى الحالة الثانية.

ومثال الجريمة الموقوفة فى نطاق المعلوماتية، أنه بينما يكون الجانى فى سبيله إلى استنفاد سلوكه، ينهض حائل يمنعه من المضى فى هذا السلوك إلى نهايته، كأن يمنعه أحد من تشغيل برامج التخريب المعلوماتى بعد أن يكون قد نشرها بالفعل.

ومثال الجريمة الخائبة أنه رغم استنفاد الجانى لسلوكه باطلاق برنامج الفيروس المعلوماتى صوب الأجهزة والبرامج المراد تخريبها، يتخلف الحدث الإجرامى المقصود وهو التخزيب المعلوماتى، إما لعدم إصابة الأجهزة المقصودة

---

(١) د/ رمسيس بهنام – مرجع سابق – ص ٦١٣.

لوجود نظم حماية فعالة، وإما يكون هذه الأجهزة والبرامج رغم وصول الفيروس المعلوماتى لها، تم التغلب عليه ولم يتم تخريبها.

كما وأن الشروع كجريمة خطر، هو فى حقيقته ليس إلا خطر وقوع الجريمة بكامل نموذجها الموصوف فى القانون، والخطر بهذا المعنى يتحقق إذا كان وقوع الجريمة محتملاً ولو احتمالاً ضعيفاً(*).

---

(*) هناك من يقول بأن صياغة القاعدة الجنائية الخاصة بالشروع، تسمح باعتبار الإنسان شارعاً ولو لم يكن قد عرض للخطر فعلاً المال موضوع الوقاية القانونية، إذ يكفى أن يكون سلوكه فى مظهره بدءاً فى تنفيذ الجريمة وأن ينطوى فى باطنه النفسى على قصد ارتكابها.

Hellmuth Mayer "Strafrech" Allgemeiner Teil. Tubingen 1967, p.143.

ولكن هذا القول يرد عليه أستاذنا الدكتور/ رمسيس بهنام بأن تفسير القاعدة الجنائية الخاصة بالشروع، العبرة فيه بالمعنى المنطقى لا بالمعنى الحرفى. فالعقاب على الشروع لم يتقرر بالإضافة إلى عقاب الجريمة التامة، إلا لأن الشروع ينذر بخطر هذه الجريمة ويعتبر بهذه المثابة جريمة خطر، وإلا فلا تقوم للركن المادى فيه قائمة، وبالتالى لا تتطابق مع نموذجها واقعة الحال.

وهناك من يرى أن عقوبة الشروع واجبة حتى فى حالة الاستحالة المطلقة لأن قانون العقوبات نظام مرسوم للسلوك البشرى، وقاعدة الشروع بدورها تدخل فى ذلك النظام وتنهى عن سلوك معين، ومن يقدم على جريمة يتبين أنها على غير علم منه مستحيلة الوقوع، إنما يتعارض سلوكه مع تلك القاعدة الناهية، والعبرة فى كل سلوك بالغاية التي يهدف إليها.

هذا الرأى ينادى به أصحاب التصوير الغائى أو الهدفى وعلى رأسهم الأستاذ Welzel، كما تأخذ به المحكمة العليا الألمانية – راجع:

Welzel Das Deutsche Strafrecht "Berlin 1969 - p. 192 et S. Jescheck "Lehrbuch des Stafrechts" Allgemeiner Teil, Berlin 1969, p. 352.

واعتراض الأستاذ الدكتور/ رمسيس بهنام على هذا الرأى أن الشروع محل عقاب لا بالنظر إلى الركن المعنوى فيه وحده، وإنما حين يتوافر كذلك ركنه المادى. ولا بد لوجود الركن المادى فى الشروع كما سلف القول من تحقق خطر فعلى على المال موضوع وقاية القانون الجنائى، حتى إذا كان هذا الخطر لا يتعدى من بين درجات احتمال إحداث الضرر بالمال ذاته، درجة الاحتمال الضعيف. وليس الشروع خطراً منبعثاً من شخص، وإنما هو خطر منبعث من سلوك.

ويذهب رأى ثالث إلى القول بأنه يكفى فى العقاب على الشروع أن يوقظ السلوك لدى مشاهدة الإحساس بأن المال موضوع وقاية القانون الجنائى، معرض للخطر، ولو لم يكن لهذا الخطر وجود فعلى.

-/-

ولا يتحقق مثل هذا الاحتمال الضعيف بوسيلة مجردة من كل صلاحية، أو سلوك يقصد به الفاعل موضوَعاً للجريمة لا وجود له في العالم الكوني. فيلزم لتحقيق احتمال حدوث الجريمة ولو بدرجة ضعيفة يوجد بها معنى خطر وقوعها، أن يتخذ الفاعل سلوكه والموضوع المقصود كائن في العالم المحيط وإن كان متخلفاً في مكان السلوك، أو أن يستخدم الفاعل وسيلة على قدر من صلاحية تحقيق النموذج الإجْرامي الموصوف قانوناً، ولو كان هذا القدر لا يكفي.

---

Mezger - Blei "Strafrecht" I. Allgemeiner Teil. München 1968. p. 244, 245. —

غير أن هذا الرأى وإن أقام وزناً لإحدى خصيصتين فى السلوك المكون للشروع، أغفل خصيصة أخرى لابد من توافرها فى هذا السلوك لقيام الشروع وهى أن ينطوى السلوك نفسه وفى ذاتيته على درجة من الخطر الفعلى على المال موضوع وقاية القانون، ولو كانت أدنى درجات الخطر.

ولقد جرت كتب الشراح على ضرب المثال لحالة يمتنع فيها العقاب ويجمع حتى الفقه الألمانى على انتفاء العقاب فيها، وهى حالة من يستخدم أساليب الشعوذة والسحر ليقتل بواسطتها إنساناً، إذ لا يتوافر فى حقه حتى شروع فى قتل.

وقيل فى تعليل استبعاد العقاب، إن مثل ذلك الشخص يعتبر من السذاجة إلى حد يجعل القصد الجنائى عنده متخلفاً. راجع:

Stefani et Levasseur "Droit pénal général et procedure pénale". t. I. 1964, N°. 186.

ويرى الاستاذ الدكتور/ رمسيس بهنام أن العقاب يستبعد فى ذلك الفرض لا لأن الركن المعنوى غير قائم، وإنما لأن الركن المادى فى الشروع ذاته غير متوافر. فقد يتحقق لدى الفاعل فى مثل تلك الواقعة قصد جنائى جدى يتمثل فى انصراف نيته حقاً إلى إزهاق روح انسان، وهذا يكفى للقول بوجود الركن المعنوى. وإنما تعد الوسيلة المستخدمة من جانبه منعدمة الصلاحية فى تحقيق الهدف الإجرامى المنشود، وبالتالى لا تقوم بها ولو درجة دنيا من درجات الخطر المنذر بأقتراف القتل، وهذا معناه عدم تحقق الركن المادى للشروع فى قتل. (د/ رمسيس بهنام – المرجع السابق – ص ٦٤٧ وما بعدها)، ويراجع : د/ سمير الشناوى – «الشروع فى الجريمة» – القاهرة – ١٩٧٠».

(ب) القصد الجنائي:

الشروع جريمة ينبغي أن يتوافر فيها الركن المادى. ولا يختلف هذا الركن الخاص بجريمة الشروع عن الركن المعنوى للجريمة التامة، إذ هما يخضعان لنفس الأحكام ويشتملان على ذات العناصر[1]. ومؤدى ذلك أن يكون السلوك الصادر عن الجانى إدارياً، وأن يتوافر علمه بكافة العناصر الواقعية الجوهرية اللازمة قانوناً لقيام الجريمة، بما يشتمل عليه ذلك من ضرورة توافر علمه بصلاحية السلوك الذى أتاه لإحداث النتيجة، وأن يتوافر لديه أيضاً نية تحقيق النتيجة، أو كما يطلق على ذلك أحياناً إرادة أو قصد تحقيق النتيجة[2].

وإذا كانت جريمة الشروع من جرائم القصد الخاص، فلابد أن يتوافر لدى الجانى هذا القصد الخاص كنية إزهاق روح إنسان حى فى جريمة القتل، ونية التملك فى جريمة السرقة. وفى نطاق الجريمة المعلوماتية[*]. يجب أن تتوافر:

- نية أختراق البيانات (الأتصالات) فى جريمة الاعتراض غير القانونى.
- نيـة الإضـرار L'endommagement أو التـعطيل Détérioration أو المحـو L'effacement أو الطمس La suppression للبيانات المعلوماتية Données in-formatiques فى جريمة الاعتداء على سلامة البيانات.

---

(١) نقض جنائى ١٦ إبريل ١٩٣٤ – مجموعة القواعد القانونية – جـ٣ – ق ٢٣٢ – ص ٣٠٩، نقض ١٢ يونيو ١٩٥٠ – مجموعة أحكام النقض – س ١ – ق ٢٤٥، ص ٧٥١، نقض ٢١ مايو ١٩٥٦ – أحكام النقض – س ٧ – ق ٢١٠ – ص ٧٤٦.

(٢) د/ سليمان عبد المنعم – النظرية العامة لقانون العقوبات – دار الجامعة الجديدة – الإسكندرية – سنة ٢٠٠٠ – ص ٦٢٠.

ورغم أن السلوك يجعل الوقوع المادى لجريمة قوى الاحتمال، قد لا يكون فى ذاته وبمفرده كافياً للكشف عن انصراف أرادة صاحبه إلى ارتكاب هذه الجريمة. (د/ رمسيس بهنام – مرجع سابق – ص ٦١٥).

(*) تم ترتيب الجرائم المعلوماتية أهتداء بما ورد فى اتفاقية بودابست ٢٠٠١ بشأن الجرائم المعلوماتية، مع الوضع فى الاعتبار تجريم هذه الأفعال بمعرفة المشرع الوطنى.

وأيضـا نيـة الإتلاف Le terme altération(*)، أو إدخـال شـفرات عـدوانيـة L'introduction de codes malveillants في ذات الجريمـة.

- نية الإعاقة Entrave التى تكون ناجـمة عن الإدخال أو النقل أو الإضرار أو المحو أو الإتلاف أو طمس البيانات المعلوماتية لوظيفة نظام الحاسب، وتعنى جـريمة تخـريب نظام الحـاسب Sabotage informatique. ويـجـب أن تـكـون الإعاقة جسيمة لترتيب الجزاء الجنائى.

- نيـة خلق Créer أو تعـديل غـير مـصـرح بـه Modifier sans autorisation للبيانات المسجلة بطريقة من شأنها أن تحوز هذه البيانات قيمة دامغة Une Valeur Probante مـخـتلفـة عن سياق المعامـلات القـانونيـة، والتـى تكون مـؤسسة على صـحـة L'authenticité المعلومـات المستـخـرجـة من خـلال هذه البيانات، وبالتالى يمكن أن تكون مـوضـوعاً لخداع d"une Tromperie. وذلك يمثل جريمة التزوير المعلوماتى.

- نيـة التـلاعـب بمدخـلات النـظام A'L'entrée du systéme – ويعنـى تغـذيـة الحـاسب ببيانات غير صـحيـحة -En introduis ant dans l'ordinateur inex actes – أو نيـة التـلاعـبـات فـى البـرامج، من أجل الحـصـول دون حق على منفعة اقتـصادية للفاعل أو للغير. وذلك يمثل جـريمة الغش المعلومـاتى الذى يسبب ضـررا أقتصادياً – مادياً – للغير.

- نيـة الإنتاج أو النشـر غير المشروع للمواد الإباحيـة الطفولية La Production ou la diffusion illicites de pornographie عـبر النظم المعلومـاتيـة Par Lebiais de Systéme informatique. والـذى يغطـى الجـــرائم المـرتـبطـة بالمحتوى.

---

(*) يعنى تغيير البيانات الموجودة La modification de données existaantes.
مثال ذلك: الفيروسات Des Virus.. التى هى عبارة عن برنامج يصممة المجرم المعلوماتى بطريقة تعطيه القدرة على ربط نفسه ذاتياً ببرامج أخرى، ثم يتوالد ويتكاثر تلقائيا وينتشر داخل البرامج المختلفة، أو بين مواقع معينة من ذاكرة الحاسب حتى يحقق الأهداف المتوخاه منه.

**(جـ) تخلف الجريمة رغم إرادة الفاعل:**

يراد بتخلف الجريمة فى هذا المجال، عدم تحقيق الصورة الكاملة لها، كما هى مرسومة فى نموذجها المحدد بالقاعدة الجنائية.

وإخفاق السلوك فى تحقيق تلك الصورة الكاملة للجريمة، يجب لاعتباره شروعا فى الجريمة ذاتها، أن يكون حادثاً رغم إرادة الفاعل. ذلك ما اشترطه القانون حين تطلب أن يكون التنفيذ قد أوقف أو خاب لأسباب لادخل لإرادة الفاعل فيها (م ٤٥ عقوبات)[1].

وذهب رأى إلى أن عدم وقوع النتيجة لسبب لا دخل لإرادة الفاعل به، يمثل العنصر الثانى للركن المادى لجريمة الشروع[*]. وهو أهم ما يميزها فى نفس الوقت عن الجريمة التامة التى لا يتصور إكتمالها قانوناً إلا بوقوع النتيجة متى كانت بطبيعة الحال من بين جرائم الحدث التى يتعين أن يتمخض عنها نتيجة. وعدم وقوع النتيجة يمثل عنصراً فى صورتى الشروع الناقص والتام. على أن أهم ما يميز هذا العنصر هو وجوب أن يكون تخلف النتيجة غير إرادى، أى راجعاً لسبب لا دخل لإرادة الفاعل به، أما إذا كان تخلف النتيجة راجعاً لسبب إرادى مبعثه أرادة الفاعل نفسه، فإننا فى هذه الحالة نخرج من دائرة الشروع المعاقب عليه لنصبح بصدد عدول إرادى Désistement Volontaire وهو يمنع من قيام جريمة الشروع ويحول بالتالى دون عقاب الفاعل[2].

فمفاد ذلك بمفهوم المخالفة، أنه حيث يكون لإرادة الفاعل دخل فى تلك الأسباب التى أوقفت التنفيذ أو خيبت أثره، لا تقوم للشروع قانوناً قائمة، ولا يستحق الفاعل عن سلوكه عقاباً[3]. ويحدث ذلك عندما يتوقف الفاعل

(١) د/ رمسيس بهنام – مرجع سابق – ص ٦١٧.

(*) حيث أن العنصر الأول للركن المادى هو البدء فى التنفيذ، والذى يعتبر الحد الايجابى للشروع.

(٢) د/ سليمان عبد المنعم – مرجع سابق – ص ٦٠٧.

(٣) د/ رمسيس بهنام – المرجع السابق.

-/-

عن المضى فى ذلك السلوك – الذى من شأنه مادياً أن يصبح نفاذ الجريمة به قوى الاحتمال – أو يحبط بنفسه النتيجة المترتبة عليه، وذلك بوازع تلقائى من إرادته.

## الفرع الثاني

## الشروع في جرائم المعلوماتية في التشريع الفرنسي

ضمن المشرع الفرنسى فى المادة ٧/٣٢٣ عقوبة الشروع فى الجرائم المنصوص عليها فى المواد من ١/٣٢٣ إلى ٣/٣٢٣ من القانون الصادر عام ١٩٩٤ المتعلق بالاعتداءات التى تقع على نظام المعالجة الآلية للمعطيات. ونظراً للذاتية الخاصة لجرائم المعلوماتية، فقد قرر المشرع أن العقوبة على الشروع فى هذه الجرائم هى نفس عقوبة الجريمة التامة(١)، وذلك بخلاف القوانين التقليدية فى التشريع العقابى المصرى، التى صاغت عقوبة للشروع تختلف عن عقوبة الجريمة التامة.

وانه أن كان هناك مراحل سابقة على ارتكاب الجريمة لا يجرمها المشرع ولا يعاقب عليها، حيث أنها مراحل لم تتخذ المظهر الخارجى ولا المظهر المادى للأفعال، فهى فى ضمير الجانى تكون نفسية مثل مرحلة التفكير ومرحلة التصميم عليها(٢)، حيث اراد المشرع بذلك تشجيع الجانى على العدول عن تنفيذ

---

ـــ ويضيف: أنه قد يدق ويصعب من الناحية العملية البت فيها إذا كان العدول عن أكمال الجريمة من جانب الشارع فيها، يعتبر راجعاً إلى إرادته أم إلى ظرف خارج عن هذه الإرادة. ونرى أن ذلك العدول يعتبر راجعاً إلى ارادة الفاعل إذا لم يكن ثمرة اضطرار ناشئ من عامل خارجى وجد فى محيط السلوك أو تخيل الفاعل وجوده.

(1) Loi du 5 Janvier 1988 relative a la fraude informatique (art 462/7). la temtative des delits prevus par les articles 4622a 462/6 est Punie des memes penes que le delit lui - meme.

(٢) د/ أحمد حسام طه – الجرائم الناشئة عن استخدام الحاسب الآلى – مرجع سابق – ص ٥٩٢.

الجريمة وعدم اتمامها. لكن هناك أفعال تخرج عن هذا السياق كما لو أعلن الجاني عن تصرفات تدل على ارادته وسلوكه الإجرامي كالتهديد أو التحريض أو الاتفاق الجنائي،فهي أفعال لها نصوص قانونية تعاقب عليها(1) .

حيث نص المشرع الفرنسي في القانون الصادر في يناير ١٩٨٨ المتعلق بالمعلوماتية بتجريم الأعمال التحضيرية في صورة الاتفاق الجنائي بنص المادة ٨/٤٦٢ وذلك من أجل تنفيذ جريمة من الجرائم المنصوص عليها في نفس القانون من المادة ٢/٤٦٢ إلى المادة ٦/٤٦٢ .. ومع التعديل الحديث لقانون العقوبات الفرنسي عام ١٩٩٤ تعدلت المادة ٨/٤٦٢ بالمادة ٤/٣٢٣، والمادة ٤٦٢ بالمادة ١/٣٢٣.

وفي هذا السياق اتجه رأى في الفقه الفرنسي إلى توسيع مفهوم الشروع باعتباره هو مقدمة الفعل غير المشروع، وبالتالي فإن الجزء الأكبر من الأعمال التحضيرية يعد داخلاً في نطاق الشروع، ويعتبرها هذا الرأى متفق مع مقصد المشرع فيما ذهب إليه عند وضع نص المادة ٨/٤٦٢ المعدلة بالمادة ٤/٣٢٣ بقانون ١٩٩٤(2) .

وحيث اتجه الفقه – يؤيده القضاء – إلى أنه لا شروع في الجرائم الشكلية، لكن بالتطبيق على جرائم المعلوماتية، وخصوصاً النص المتعلق بالشروع الصادر في المادة رقم ٧/٣٢٣ بالقانون ١٩٩٤ المتعلق بجرائم الغش المعلوماتي، حيث ينص على العقاب في حالة الشروع بنفس عقوبة الجريمة التامة، الجرائم المنصوص عليها بالمادة ١/٣٢٣ حتى المادة ٣/٣٢٣.

Art 323/7: "La tentative des delets Prets par lis articles 323 - 1 a 323 - 3 Punie des memes Peints.

---

(١) يعاقب المشرع المصري على التحريض في نص المواد (٩٥ – ٩٧ – ١٧٣ عقوبات)، ويعاقب على الاتفاق الجنائي في نص المادة (٤٨ – ٩٦ عقوبات)، ويعاقب على التحريض في نص المادة (٣٢٧ عقوبات).

(٢) د/ أحمد حسام طه – المرجع السابق – ص ٥٩٦.

ومن الملاحظ أن المشرع الفرنسى فى مشروع القانون المتعلق بالمعلوماتية، قد غلظ العقوبة للشروع وجعلها نفس عقوبة الجريمة التامة، حيث أنه عند مناقشة النص رأى اختلاف ما بين الجرائم التقليدية وجرائم الحاسب الآلى، باعتبار أن الأخيرة لها ذاتية خاصة، وطرق فنية يتبعها المجرم المعلوماتى، تختلف عن الطرق المتبعة فى الجرائم العادية، فاعتبر المشرع أن الشروع فى الجريمة المعلوماتية يعاقب عليه بنص العقوبة المقررة للجريمة التامة(١).

ومثال لذلك جريمة الدخول فى شبكة معلوماتية التى جرمها المشرع الفرنسى بنص المادة ٣٢٣/١ من القانون ١٩٩٤، وقد اعتبرها جريمة شكلية إلا أنه عاقب عليها بعقوبة الجريمة التامة حال الشروع فيها. ولأنها جريمة شكلية لا يتطلب لتمامها نتيجة معينة حيث اعتبر المشرع أن مجرد الدخول جريمة فى حد ذاتها، ثم إذا تلتها جرائم أخرى فيكون ذلك ظرف مشدد.

## الفرع الثالث

## الشروع في الجريمة المعلوماتية طبقاً للاتفاقيات والمعايير الدولية الحديثة(٢)

ضمت اتفاقية بودابست ٢٠٠١ المتعلقة بالإجرام الكونى Convention sur la cyber criminalité, Budapest, 23, x1.2001 بمعنى الإجرام المعلوماتى أو الجرائم المعلوماتية، بين نصوصها فى الفصل الخامس المعنون (أشكال أخرى

---

(١) المرجع السابق – ص ٦٠٣.
تختلف الجريمة المعلوماتية كثيراً فى خصوصيتها ووسائلها عن الجريمة العادية، وكذلك فى سرعة تنفيذها بالضغط على مفاتيح Kay الحاسب لتكون النتيجة باسرع وقت ممكن، وقد تكون الجريمة بوضع برنامج تظهر نتيجة وآثاره بعد وقت. المهم أن المشرع تلاشى الصعاب والمتاعب التى قد يتعرض لها القضاء عند البحث عن توافر الشروع فى هذه الجريمة، فنص على عقوبة الجريمة التامة عند توافر حالة الشروع.

(٢) للمزيد بشأن الفصل الخامس من إتفاقية بودابست ٢٠٠١ يراجع:
د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية الإجرائية لجرائم المعلوماتية(على ضوء اتفاقية بودابست ٢٠٠١) – مرجع سابق – ص ص ١٤٣ – ١٥٥.

للمسئولية والجزاءات (Autres Formes de respnsabilité et de sanctions) – المادة (١١) التى تعالج الشروع فى فقرتها الثانية ونصها كما يلى(*):

- يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم – وفقاً لقانونه الداخلى – كل شروع عمدى لارتكاب إحدى الجرائم المشار إليها فى المواد ٣–٥، ٧، ٨، ٩ (فقرة ١ – أ، جـ) من الاتفاقية الحالية.

وتبين المذكرة التفسيرية أن الهدف من هذه المادة إنشاء جرائم تكميلية Des infractions supplémentaires ترتبط بالشروع فى ارتكاب الجرائم المعرفة بواسطة هذه الاتفاقية – والسابق بيانها – بغرض تجريم هذه الأفعال.

وبعض الجرائم المُعرفة فى هذه الاتفاقية أو بعض عناصر هذه الجرائم يصعب تصور الشروع فيها. كما هو الحال فى العناصر المتعلقة بواقعة تقديم أو إتاحة المواد الإباحية الطفولية Offrir ou rendre disponible de la pornographie enfantine. وعلاوة على ذلك فإن بعض النظم القانونية قد حددت الجرائم التى يكون فيها الشروع معاقباً عليه(**).

وكما هو الحال فى سائر الجرائم المنصوص عليها بمقتضى هذه الاتفاقية، فإن الشروع يجب أن يتم ارتكابه عمداً Intenionnellement.

---

(*) النص الفرنسى لهذه الفقرة: - Article 11 - Tentative et complicité:

2- Chaque Partie adopte les mesures législatives et autres qui se révélent nécessaires pour ériger en infraction Pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des Articles 3 à 5, 7, 8, 9 (1) a et 9 (1) c de la présente convention.

(**) وتأسيساً على ذلك فإن الأطراف لا يلتزمون بتجريم الشروع إلا فى الجرائم المحددة فى المواد الآتية:

| | |
|---|---|
| المادة (٣) الاعتراض غير القانونى | - Interce-ption illégale |
| المادة (٤) الاعتداء على سلامة البيانات | - Atteinte à l'intégrité des données |
| المادة (٥) الاعتداء على سلامة النظام | - Atteinte à l'intégrité du systéme |
| المادة (٧) التزوير المعلوماتى | - Falsification informatique |
| المادة (٨) الغش المعلوماتى | - Fraude informatique |

=/=

## المطلب الثاني

## الاشتراك في الجريمة المعلوماتية

### الفرع الأول

### الوضع في التشريع الوطني

المساهمة الأصلية في الجريمة تعني أن يكون للمساهم دور رئيسي في تنفيذ الجريمة، سواء منفرداً حين يضطلع بتنفيذ الجريمة بنفسه ويسمى في هذه الحالة بالفاعل المنفرد، أو بالإشتراك مع غيره إذ يقومان بتنفيذ الجريمة معاً ويطلق عليه في هذه الحالة الفاعل مع غيره، وفي الحالتين تكون هذه المساهمة الأصلية مادية[1].

وفي هذا الشأن عرف الأستاذ الدكتور/ أحمد فتحي سرور الفاعل بأنه من يقوم في تنفيذ الجريمة بدور «البطولة»، أما الشريك فقد عرفه بأنه من يقوم في تنفيذ الجريمة بدور «الكومبارس»[2].

---

== المادة (٩) الجرائم المتصلة بالمواد الإباحية للأطفال - Fraude informatique

فقرة: ١- يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأيه إجراءات أخرى يرى أنها ضرورية لتجريم - تبعاً لقانونه الداخلي - السلوكيات التالية إذا ارتكبت عمداً ودون حق:

أ - إنتاج مواد إباحية طفولية بغرض نشرها عبر نظام معلوماتي.

ب- تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتي.

جـ- النشر أو النقل لمادة إباحية طفولية عبر نظام معلوماتي.

(١) د/ سليمان عبد المنعم - مرجع سابق - ص ٦٣٣.

- ولكن قد يضطلع الشخص أيضا بدور رئيسي أو أصلي في تنفيذ الجريمة ويعتبر فاعلاً لها إذا حرض ودفع شخصاً آخر حسن النية أو ممن تمتنع مسؤوليتهم الجنائية إلى ارتكاب الجريمة على نحو يعتبر هو فيه الفاعل المعنوى (الحقيقى) للجريمة بينما من قام بتنفيذها لا يعد أكثر من أداة تنفيذية، وتكثر صور هذه الحالة في جرائم التزوير المعلوماتي كمن يوهم معد البرامج المعلوماتية بصحة بيانات خاصة به على غير الحقيقة، بتسجيلها عبر قنوات شرعية رسمية للنظم المعلوماتية، لاستغلال هذه البيانات في أعمال مشبوهة أو ارتكاب أفعال غير مشروعة اعتماداً عليها، فمن أملى هذه البيانات هو الفاعل المعنوى في جريمة التزوير، أما محرر هذه البينات الذى أثبتها في النظام المعلوماتي فليس فاعلاً للجريمة ولا مساهماً فيها لحسن نيته.

(٢) د/ أحمد فتحي سرور - الوسيط في قانون العقوبات (القسم العام) - دار النهضة العربية - سنة ١٩٨٥ - ص ٥١٣.

وذهبت محكمة النقض فى حكم لها إلى أن الاشتراك كما هو معروف به فى القانون، اتحاد نية أطرافة على ارتكاب الفعل المتفق عليه، ويتم غالباً دون مظاهر خارجية أو أعمال مادية محسوسة يمكن الاستدلال عليها(١).

وقد نصت المادة ١/٣٩ من قانون العقوبات المصرى على أنه: «يعد فاعلاً للجريمة:

أولاً: من يرتكبها وحده أو مع غيره.

ثانيا: من يدخل فى ارتكابها إذا كانت تتكون من جملة أعمال فيأتى عمداً عملاً من الأعمال المكونة لها»

ويستخلص من ذلك أن المساهم الأصلى فى الجريمة إما أن يكون فاعلاً ينفرد بتنفيذ الجريمة وحده، أو يتولى تنفيذها مع غيره(*).

فالفاعل إذن هو من يتحقق بسلوكه نموذج الجريمة الموصوف فى القانون، تحقيقاً كلياً أو جزئياً(**).

أما الشريك فهو من يساهم فى الجريمة بسلوك خارج عن الوصف الوارد فى نموذجها، وإن كان مرتبطاً بالسلوك الموصوف فى هذا النموذج ومتصلاً به لكونه اتفاقاً أو تحريضاً أو مساعدة عليه.

---

(١) نقض ١ فبراير ١٩٦٠ – مجموعة أحكام النقض – س ١١ – رقم ٢٢ – ص ١١٢.
وقضت محكمة النقض فى ذات الحكم بأن للقاضى الجنائى إذا لم يقم على الاشتراك دليل مباشر من اعتراف أو شهادة شهود أو ما أشبه. أن يستدل عليه بطريق الاستنتاج من القرائن التى تقدم لديه مادام هذا الاستدلال سائغاً وله فى ظروف الدعوى ما يبرره.

(*) حين يتعدد الأشخاص الذين تقع الجريمة بسلوكهم، يمكن التمييز بينهم بحسب ما إذا كان سلوك الواحد منهم يحقق نموذج الجريمة الموصوف فى القانون أو على الأقل جزءاً من هذا النموذج، أو يتخذ على العكس مظهراً خارجاً عن الوصف المرسوم للجريمة فى نموذجها. ذلك لأنه فى الحالة الأولى يسمى الشخص المساهم فى الجريمة باسم الفاعل، بينما يسمى فى الحالة الثانية باسم الشريك. (د/ رمسيس بهنام – مرجع سابق – ص ٦٤٨).

(**) يلاحظ أنه حتى الشروع يعتبر تحقيقاً لنموذج جريمة ناقصة هى بالذات جريمة الشروع – وبديهى أن نموذج جريمة الشروع وضعه من نموذج الجريمة التامة، أنه بدء فى تنفيذ النموذج الأخير أى تحقيق جزئى له.

ولم يخرج المشرع عن ذلك المعنى فى صياغة المادة (٣٩ع) المتضمنة تعريفها للفاعل، ولا المادة (٤٠ع) فى تعريفها للشريك والتى نصت على أنه:
«يعد شريكاً فى الجريمة:

أولاً: كل من حرض على ارتكاب الفعل المكون للجريمة، إذا كان هذا الفعل قد وقع بناء على هذا التحريض.

ثانياً: من اتفق مع غيره على ارتكاب الجريمة فوقعت بناء على هذا الاتفاق.

ثالثاً: من أعطى للفاعل أو للفاعلين سلاحاً أو آلات أو أى شئ آخر مما استعمل فى ارتكاب الجريمة مع علمه بها، أو ساعدهم بأى طريقة أخرى فى الأعمال المجهزة أو المسهلة أو المتممة لارتكابها»(*).

(*) يلزم لاعتبار الجريمة واقعة من عدة أشخاص رغم وحدتها، أن يكون بين هؤلاء رباط معنوى يجمع بينهم فى جريمة واحدة، وإلا تعددت الجريمة بتعددهم ونسبت إلى كل منهم جريمة متميزة.

وليس بلازم فى هذا الرباط المعنوى أن يتخذ صورة التفاهم السابق بين أكثر من شخص على ارتكاب الجريمة.

فتعتبر جريمة السرقة واحدة، ولو تصادف أو وجد أكثر من سارق واحد فى مكان ما دون تفاهم سابق بينهم على السرقة من هذا المكان. ذلك لأن الرباط المعنوى الجامع بينهم فى سرقة واحدة يتحقق فور تلاقيهم فى مكان السرقة وإحساس كل منهم بوجود الآخر معه، وانصراف إرادته فى تلك اللحظة بالذات إلى ما يتطابق مع إرادة هذا الآخر، ولو لم ينعقد بينهم قرار مشترك حول توزيع حصيلة السرقة فيما بينهم. فعلى الرغم من عدم وجود اتفاق سابق يتفاهم به المساهمون على ارتكاب جريمة معينة، يكفى أن يطرأ بينهم هذا الاتفاق أثناء تنفيذ الجريمة، وفى أية لحظة من لحظات هذا التنفيذ تسبق نهايته، كى تقوم رابطة ذهنية معنوية تحقق بين المساهمين الاتفاق على ذات الجريمة الجارى تنفيذها. (د/ رمسيس بهنام – المرجع السابق – ص ٦٥١).

على أنه ليس بلازم فى كل توافق أن يكون اتفاقاً، فقد تتوارد الخواطر صوب هدف ما، بينما البعض منها منصرف إلى هدف أبعد، فلا يوجد بينها اتفاق على الهدف الآخير، فيما لو تحقق، أى يتوافر بين الخواطر اتفاق على الهدف الأول بينما يتخلف بينها هذا الاتفاق بشأن الهدف الثانى. (نقض ١٩ أكتوبر ١٩٦٥ – مجموعة القواعد القانونية – س ١٦ – رقم ١٣٦ – ص ٧١٨). حيث حدث أن عدة أشخاص تشاجروا مع آخرين فى السوق، وتوافقوا بعد بلوغ منازلهم على العودة إلى السوق حاملين البنادق للانتقام، واطلق بعضهم أعيرة نارية قضت على بعض

-/-

وإذا كان التفاهم متوافراً حتماً وبحكم طبيعة الأمور فى حالتى الاتفاق والتحريض، فإن المساعدة من المتصور أن تتم بدونه.

والواقع أن المساعدة على الجريمة تحقق الاشتراك فيها، دون تفاهم مع فاعل الجريمة من جانب من قدم المساعدة. ولو كان التفاهم على المساعدة لازم قانوناً فى سبيل أن يعتبر مقدمها شريكاً فى الجريمة، لما كانت هناك حاجة تدعو إلى أن يفرد القانون للمساعدة ذكراً خاصاً إلى جانب ذكره للاتفاق والتحريض، ولصار فى هذين غناء عنها، تبعاً لكون التفاهم على المساعدة يجعل منها اتفاقاً أو تحريضاً(١).

هذا والاتفاق الذى يجمع بين فاعلين متعددين، من شأنه أن يجعل نشاطهم وحدة متكاملة، تعزى إليهم كلهم، وينسب سلوك كل منهم فى تنفيذ الاتفاق لا إلى صاحبه فحسب، وإنما إلى سائر المساهمين معه فى ذات التنفيذ باعتباره هدفاً مشتركاً عبؤه واقع عليهم جميعاً، فالطعنة القاتلة مثلاً تنسب إلى كافة الطاعنين المنفذين للقتل، حتى إلى من كان منهم قد طعن فى غير مقتل(٢).

- عناصر الاشتراك:

يستفاد من نص المادة ٤٠ عقوبات فى تعريفها الشريك، أنه تلزم لتوافر الاشتراك عناصر ثلاثة:

---

= الخصوم، وإذ أدانتهم محكمة الجنايات بوصفهم جميعاً - من أطلق منهم النار ومن لم يطلقها - فاعلين فى القتل - خطأت محكمة النقض هذا الحكم لأنه وإن وجدت بين المتهمين رابطة ذهنية فى خصوص الانتقام، لم يثبت وجود هذه الرابطة بينهم فى خصوص القتل، فكان القول باتفاقهم على القتل غير قائم على أساس.

(١) نقض ٣٠ مايو ١٩٥٠ - مجموعة القواعد القانونية - س ١ - رقم ٢٣٠ - ص ٤٠٩، نقض ٨ أبريل ١٩٥٢ - مج - س ٣ - رقم ٣٠٣ - ص ٥٨٠.

(٢) د/ رمسيس بهنام - المرجع السابق - ص ٦٥٥.

وبناء على ذلك حكم بأنه متى كان المتهمون مسئولون جميعاً عن النتيجة لاتفاقهم عليها، فلا يكون لازماً تحديد من منهم محدث الاصابات التى أدت إلى وفاة المجنى عليه. (نقض ٢٨ نوفمبر ١٩٦١ - مج - س ١٢ - رقم ١٩٢ - ص ٩٣١).

١- أن يتخذ سلوك المتهم صورة من الصور التى وصف القانون بها سلوك الشريك، وهى الاتفاق أو التحريض أو المساعدة.

• الاتفاق: فمعناه التلاقى بين إرادتين كانت كلتاهما منصرفة إلى إرتكاب الجريمة (*). ومن صور الاتفاق سبق الإصرار بمعنى أن ثبوت سبق الإصرار فى حق المتهمين، يستلزم بالضرورة توافر الاشتراك بالاتفاق بالنسبة لمن لم يقارف الجريمة بنفسه منهم(١).

• التحريض: هو العمل على انعقاد إرادة إجرامية لدى شخص لم يكن قد كونها بعد، حتى أنه بدون ذلك العمل ما كانت تصح عليها نيته من تلقاء نفسه(**).

• المساعدة: هى امداد فاعل الجريمة بسلاح، أول آلة أو أى شئ آخر، كما يقرر نص المادة ٤٠ ف ٣ عقوبات.

٢- أن يتوافر لدى المتهم فى إتيانه هذا السلوك، قصد الإسهام فى جريمة معينة تنفذ على يد غيره.

ولا شك أنه لاعتبار قصد الاسهام فى الجريمة قائماً، يجب مبدئياً العلم بهذه الجريمة وموضوعها على وجه التحديد.

٣- وقوع الجريمة بناء على سلوك الشريك.

لابد لاعتبار المتهم شريكا فى جريمة ما، أن تقع هذه الجريمة فعلاً بناء

---

(*) هذا التلاقى كفيل بأن يقطع دابر التردد الذى كان من المحتمل أن يصيب كلا من صاحبيهما، لو كان فى عقده للنية الإجرامية وحيداً.

(١) نقض ١٣ مارس ١٩٧٨ – مج س ٢٩ – رقم ٥٢ – ص ٢٧٥.

(**) تقضى المادة ١٧١ ع بأن تحريض شخص أو أكثر علناً على ارتكاب جناية أو جنحة، يعتبر اشتراكاً فيها إذا وقعت – بينما لا تشترط العلانية فى التحريض الوارد بنص (م ٤٠ ع). وأيضاً يمتد ليشمل المخالفات.

على اتفاقه أو تحريضه أو مساعدته عليها، فإذا أتفق عليها دون أن تقع لا يعتبر شريكاً فيها، ولا يمكن أن يعاقب بعقوبتها(*) .

## الفرع الثاني

## الاتفاق الجنائي المعلوماتي في التشريع الفرنسي

نصت المادة ٤/٣٢٣ من قانون العقوبات الفرنسي الجديد على أنه: «كل من ساهم فى جماعة مشكلة أو فى اتفاق من أجل التحضير المصحوب بفعل أو عدة أفعال مادية من أجل تنفيذ جريمة أو عدة جرائم من الجرائم المنصوص عليها فى المواد ١/٣٢٣ حتى المادة ٣/٣٢٣. يعاقب بالعقوبة المنصوص عليها فى الجريمة ذاتها أو بعقوبة الجريمة الأشد فى حالة تعدد الجرائم» .

ويلاحظ أن النص المتعلق بجرائم المعلوماتية يشدد فيه المشرع العقوبة لكونه يبغى الردع، ردع مرتكب الجريمة المعلوماتية التى تقدر خسائرها بالمليارات. فخروجاً على القواعد العامة التى لا تجرم الأعمال التحضيرية جرم المشرع الفرنسى فى هذا النص الأعمال التحضيرية المتعلقة بالجرائم المنصوص عليها فى هذا القانون(**) .

وقد حدد المشرع الفرنسى فى النص المتعلق بالمعلوماتية الاتفاق باعتباره مساهمة، حيث ذكر.. كل من ساهم..» ويتضح بذلك أنه قد جرم الأتفاق واتجه

---

(*) ويلزم كذلك كى يعتبر المحرض على الجريمة شريكاً فيها أن تقع الجريمة بناء على تحريضه، وأن يكون بينها وبين هذا التحريض أتصال المسبب بالسبب. (د/ رمسيس بهنام – المرجع السابق – ص ٦٦٣) .

(**) بقيام المشرع بوضع هذا النص محاولاً تفادى مشكلات الشروع فى الجريمة، وتحليل ما يدخل فى الأعمال التحضيرية وما هو فى البدء فى التنفيذ، فالاتفاق الجنائى صورة من صور الاشتراك فى الجريمة، والتحريض وسيلة من وسائل المساهمة التنفيذية فى الجريمة، فهو تدخل فى تنفيذ الجريمة بتحريض الغير على ارتكابها، ولم يحدد القانون وسائل التحريض فهى متروكة لتقدير القاضى، ويكفى فى التحريض أن يحث الفاعل على تنفيذ الجريمة، ولم يشترط أن يكون هو صاحب فكرة الجريمة. (د/ أحمد حسام طه – مرجع سابق – ص ٦٠٩) .

وأيضا يراجع: نقض جنائى أول ابريل ١٩٣٥ – مجموعة القواعد القانونية – رقم ٣٥٤ – ص ٤٥٦، نقض ٢٨ مايو ١٩٤٥ – جـ٦ – رقم ٥٨٣ – ص ٧١٩، نقض ٢٧ ديسمبر ١٩٧٠ – مج – س ٢١ – رقم ٣٠٢ – ص ١٢٥ .

إلى الأعمال التحضيرية فادخلها فى العقاب على أنها لا تجرم فى القوانين التقليدية – كما سبق وذكرنا فى الشروع –، كما أوضح المشرع أن الاتفاق يكون مصحوباً بفعل مادى لتنفيذ واحدة من الجرائم المشار إليها أو أكثر.

وقد ذهب رأى إلى أن الاتفاق الجنائى جعل له المشرع نص خاص فى المادة ٣٢٣/ ٤، وحدد فيه الجرائم المعاقب عليها، ولا يجرم الاتفاق بالنسبة لجرائم أخرى فى المعلوماتية لم ينص عليها فى هذا القانون، حيث أن النص الفرنسى واضح فى هذا الأمر بقول المشرع: «... من أجل تنفيذ جريمة أو عدة جرائم منصوص عليها فى المواد من ٣٢٣/١ إلى ٣٢٣/٣...»(١).

## الفرع الثالث

## الاشتراك في الجريمة المعلوماتية طبقاً للاتفاقيات الدولية

اشتمل الفصل الخامس من اتفاقية بودابست بشأن الجرائم المعلوماتية(*)، على بنود إضافية Des dispositions supplémentaires بخصوص الاشتراك Complicité والشروع والجزاءات أو التدابير وذلك طبقاً للاتفاقيات أو المعايير الدولية الحديثة. وتتوزع هذه الموضعات على ثلاث مواد، تنصب دراستنا للاشتراك على قصر تناولنا للمادة (١١) من اتفاقية بودابست، والتى تنص فقرتها الأولى على أنه(**):

---

(١) د/ أحمد حسام طه – المرجع السابق – ص ٦١١. (ونتفق معه فى ما ذهب إليه، حيث أن المشرع الفرنسى واضح فيما نص عليه فى م ٣٢٣/ ٤ من القانون ١٩٩٤).

(*) إيماناً من الدول الأعضاء فى المجلس الأوروبى والدول الأخرى الموقعه على اتفاقية بودابست فى ٢٣ نوفمبر ٢٠٠١.. بالتغيرات العميقة التى حدثت بسبب الرقمية La numérisation، ويقابل هذا فى الطبعة الإنجليزية The digitalisation وهذه الكلمة مشتقة من Digit وتعنى ماهية الشئ حين يعبر عنه بالنظام الثنائى بدلاً من صور التعبير المعتادة التناظرية Analog، والاتصالات الرقمية هى نقل الإشارات بعد تحويلها للصورة الرقمية بدلاً من نقلها كموجات تناظرية. (د/ عبد الحليم شوشة – الإلكترونيات وتطبيقاتها فى الاتصالات والحاسبات والتحكم – مركز الأهرام للترجمة والنشر – القاهرة – سنة ٢٠٠٢ – ص ١٠٨).

(**) راجع باللغة الفرنسية المذكرة التفسيرية لاتفاقية بودابست ٨ نوفمبر سنة ٢٠٠١.

"Convention sur la cybercriminalite" Steno, 185, Rapport expleicaif, adopté le 8 Novembre 2001, pp. 21 ets.

–/–

«يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم – تبعاً لقانونه الداخلى – كلَ اشتراك إذا تم عمداً بغرض ارتكاب إحدى الجرائم المشار إليها فى المواد ٢ – ١٠ من الاتفاقية الحالية، بنية ارتكاب تلك الجريمة».

وتبين المذكرة التفسيرية هدف وضع هذه المادة وهو إنشاء جرائم تكميلية ترتبط بالاشتراك فى الجرائم المعرفة بواسطة هذه الاتفاقية بغرض ارتكابها.

وبالنسبة للفقرة الأولى من المادة (١١) من الاتفاقية، تلزم الأطراف بتجريم كل فعل اشتراك Tout acte de complicité بغرض ارتكاب إحدى الجرائم المنصوص عليها بمقتضى المواد من ٢ إلى ١٠ من هذه الاتفاقية، وتنشأ المسئولية الجنائية فى حالة الاشتراك إذا الشخص الذى ارتكب جريمة منصوصاً عليها فى هذه الاتفاقية تمت مساعدته بواسطة شخص آخر لديه أيضا نية ارتكاب الجريمة[1].

ومن الأمثلة التى تدل على ضرورة توافر نية ارتكاب الجريمة لدى الشريك المثال الذى أوردته المذكرة التفسيرية، والذى مفاده أن النقل La transmission عبر الإنترنت للبيانات المتعلقة بمحتوى ضار Un contenu nuisible، أو كود

— وراجع باللغة الانجليزية مسودة المذكرة التفسيرية لاتفاقية بودابست ستراسبورج ١٤ فبراير سنة ٢٠٠١.

- "Draft Explanatory Memorandum to the draft convention on cyber-crime" strasbourg, 14 February, 2001.

وراجع أيضاً المسودات التالية:

- Council of Europe draft convevtion on cyber - crime, October 2, 2000.
- Council of Europe draft convevtion on cyber - crime, november 26, 2000.
- Council of Europe draft convevtion on cyber - crime, December 25, 2000.

(١) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ١٤٦.

عدوانى Un code malvillant ، كل ذلك يتطلب مساعدة مقدمى الخدمات -Four nisseurs de services كوسطاء Comme intermédiaires فإذا لم يكن لدى مقدم الخدمة النية الإجرامية Intention criminelle، فإنه لا يكون مسئولاً فى ظل هذا القسم Au titre de cette section، ومن هذا المنطلق رتبت المذكرة التفسيرية نتيجة مؤداها أن مقدمى الخدمات ليس عليهم التزام المراقبة بهمة Surveiller activement لمحتوى Le contenu ما يعرض على شبكة الإنترنت من أجل تفادى المسئولية الجنائية بمقتضى هذا النص

- Pour eviter la responsabilité pénale en vertu de cette disposition.

الفصل الثاني

# الجريمة المعلوماتية في القانون

- المبحث الأول: تقسيم جرائم المعلوماتية.

  المطلب الأول: التقسيم الفقهي لجرائم المعلوماتية.

  المطلب الثاني: التقسيم الدولي لجرائم المعلوماتية.

  المطلب الثالث: الوضع في مصر بالنسبة لتقسيم جرائم المعلوماتية.

- المبحث الثاني: التنظيم القانوني للجريمة المعلوماتية.

  المطلب الأول: الطبيعة القانونية للمعلوماتية.

  المطلب الثاني: النصوص القانونية لحماية المعلوماتية.

# الفصل الثاني
# الجريمة المعلوماتية في القانون

فى نطاق التقنيات الحديثة أضحت العمليات التجارية والصناعية والمالية، ويضاف إليها الأتصالات والبرمجيات تعتمد على تكنولوجيا المعلومات بشكل أكثر تزايد، وفى ذات الوقت فإن الصلة المشتركة بين أنظمة تكنولوجيا المعلومات، وتحول هذه التكنولوجيا تجاه مكونات الآلات الصناعية والبرامج والأنظمة الفرعية، يؤدى إلى أضعاف أنظمة هذه التكنولوجيا بشكل متزايد أمام الهجمات الضارة، ويتضح ذلك من خلال المخاوف الخطيرة التى تسببها حالياً ما تبقى من فيروسات (عام ٢٠٠٠)، ومن الأهمية أن نعنى بالأثار الأصعب التى تخلقها (الجرائم المعلوماتية)، حيث تسعى الأنشطة الضارة التى يمارسها (القراصنة) أو المنظمات إلى استغلال أو تخريب النظام التكنولوجى المعلوماتى، أو لأفساد هذه الأنظمة، أو الحصول على ربح مالى، أو لأجل دوافع أكثر فساداً[(١)].

ولا يمكن أن نعتبر أن الجرائم المعلوماتية موجهه بشكل منفصل إلى أنظمة فردية، وذلك يرجع إلى التنامى المتسارع للصلات المشتركة بين أنظمة تكنولوجيا المعلومات. ويتم هذا عبر الشبكات الداخلية، والشبكات الإضافية، وشبكة الأنترنت ذاتها، إضافة إلى التواصل المشترك المادى المباشر أو المواد الإعلامية المخزنة القابلة للتبادل مثل ديسكات الكمبيوتر. وتقوم هذه الوصلات المشتركة – غالباً بشكل غير مقصود ونادراً ما يكون ذلك مخطط بشكل مناسب – بتحويل أنظمة تكنولوجيا المعلومات المنفصلة إلى مكونات لنظام فائق ضخم، والذى يكون معرضاً لأن يعانى الفشل التام، أو يمكن أن يتم تلويث بياناته أو برامجه بشكل خطير كنتيجة لهجمة ضارة مفردة (أو حادث).

وفى الواقع أنه مع نمو التحويل الالكترونى للأموال وجلب الأموال فى الوقت

---

(١) بحث مقدم من: بى جلادمان وآخرون – بعنوان حماية أنظمة تكنولوجيا المعلومات ضد الجريمة المعلوماتية – المؤتمر الدولى السادس للجرائم المعلوماتية – أكاديمية الشرطة – القاهرة، ١٣ :١٥ أبريل ٢٠٠٥ – ص ١١٥.

لمحدد، والهندسة المتزامنة... إلخ، غالباً ما تصبح البنية التحتية المعلوماتية لخاصة بأية منظمة أو شركة عرضه لخطورة التحول إلى جزء مصاب من نظام عالمي مصاب بأكمله، والذى يخرج تصميمه وتشغيله عن نطاق أية سيطرة كاملة فعالة(١).

وفى أطار الحد من جرائم المعلوماتية، فقد أدى الاستخدام المتزايد للبروتوكولات وواجهات البرامج القياسية لتوفير مزايا كبرى لمجتمع المستخدمين، إلا أنه فى ذات الوقت – وعلى الرغم من هذا الحرص – سهل ذلك الأمر عمليات الدخول الأولى لقراصنة المعلومات، كما أدى كذلك إلى إنتشار واسع النطاق لإستخدام قواعد البيانات المعيارية، ولوائح النشر وغيرها من تطبيقات ومكونات البرامج التطورية، وأجهزة المعالجة المعيارية، مع التطور والانتشار المستمر لأدوات وتقنيات القراصنة، كل ذلك أدى إلى جعل إختراق (المهاجم) بعمق لأنظمة المعلومات أكثر سهولة. وإضافة لذلك فإن هذه الهجمات يصعب اكتشافها، بل والأصعب هو تعقب مصادرها، ويمكن لمن يقوم بالقرصنة أن يعمل من موقع بديل بحيث يكون فى مأمن من الخضوع للعقوبة القانونية(*).

---

(١) المرجع نفسه – ص ١١٦.

(*) على سبيل المثال.. فقد أفادت تقارير صادرة من وزارة الدفاع – الولايات المتحدة – عن شن ٢٥٠,٠٠٠ ألف هجوم على الأقل ضد أجهزة الحاسب الآلى بوزارة الدفاع الأمريكية خلال عام ١٩٩٥ فقط (ويحتمل أن يكون العدد أكثر من ذلك، حيث يصعب تقدير عدد الهجمات)، وقد نجحت نسبة ٦٥٪ من الهجمات التى تم التعرف عليها. وذلك منذ فترة زمنية، فما بالنا فى الوضع الحالى، لا شك فى ازدياد هذه الهجمات أضعاف ما سبق.

- أفادت تقارير عن شن هجوماً قامت به مجموعة من القراصنة – ألقى القبض عليهم وتمت إدانتهم بتهمة اختراق أجهزة الحاسب الآلى بمؤسسات اقتصادية – شمل بنك شهير أمريكى، ومؤسسات ساوث ويسترن بيل، ومارتن مارتيا، و TRW للخدمات المعلوماتية، وكذلك بيع المعلومات – مثل تقارير الأرصدة – التى حصلوا عليها من خلال عمليات القرصنة.
- كان هناك توجه دفاعى بالمملكة المتحدة للتقليل من شأن أو انكار خطورة الجريمة المعلوماتية، والتزام الهدوء إزاء الوقائع المسببة للحرج. وعلى الرغم من ذلك فقد كان هناك عدد كاف من الحوادث التى اعترف (علانية) المسئولين لابراز التهديد الذى تمثله الجريمة المعلوماتية ضد المجتمعات.

(مناقشات المؤتمر الدولى السادس للجرائم المعلوماتية – مرجع سابق – ص ١١٧).

وتزداد عظم الخطورة المحتملة التى تمثلها الجريمة المعلوماتية، إذا ما أثرت على الأنظمة المعلوماتية الحيوية الخاصة بالاتصالات، أو توزيع الطاقة، أو أنشطة البنوك، أو بصفة عامة التطبيقات الإنتاجية والحياتية التى تستخدم النظم المطمورة، وذلك يعنى البنية التحتية المعلوماتية التى تعتمد عليها الشركات أو المؤسسات أو الأفراد(*).

**وسوف تنقسم دراستنا للجريمة المعلوماتية في القانون إلي مبحثين، بيانهما:**

**المبحث الأولي: تقسيم جرائم المعلوماتية.**

نعرض فيه للتقسيم الفقهى والدولى لجرائم المعلوماتية، ثم الوضع فى مصر بالنسبة للاجتهادات المسطرة لتقسيم الجرائم المعلوماتية.

**المبحث الثاني: التنظيم القانوني للجريمة المعلوماتية.**

نعرض فيه للطبيعة القانونية للمعلوماتية، ثم نوضح النصوص القانونية المشرعة لحماية المعلوماتية.

---

(*) بالنسبة لجرائم المعلوماتية التى تستهدف البنية التحتية، باستخدام جهاز كمبيوتر مسروق يشتمل على ناقل إشارات لاسلكية، تمكن فنى (فاتيك بودن) من تحويل سيارته إلى مركز لقيادة عمليات القرصنة واقتحم (مركز معالجة الصرف) - فى أحد ولايات أمريكا - وسرب مئات الآلاف من أطنان الصرف والمخلفات داخل الحدائق العامة وفى الانهار... كما تمكن من السيطرة على محابس التحكم فى مياه الشرب، وكان بإمكانه أن يعمل ما يحلو له فى مياه الشرب النقية لحى بأكامله. (المرجع السابق - ص ٦٥).

# المبحث الأول
## تقسيم جرائم المعلوماتية

يعد الأساس الذى ترتكز عليه الاتجاهات المتعددة فى تقسيم جرائم المعلوماتية، هو بيان الموضوعات والأنشطة الإجرامية التى تدخل ضمن إطار جرائم المعلوماتية، وقد أرسى ذلك العديد من المؤسسات والهيئات المعنية بهذه الجرائم، وأيضاً الاتجاهات الفقهية التى أدلت بدلوها فى ذات السياق، وقد استرشدت بهذا النهج العديد من التشريعات الجنائية عند إصدارها لقوانين تجرم بها تلك الأنشطة. التى تستهدف نظم المعلوماتية.

ويقصد بتقسيم جرائم المعلوماتية، تمييز كافة صور الأفعال غير المشروعة المرتبطة بالنظم المعلوماتية، ودراسة كل نوعية منها بشكل مستقل، بقصد تجميع وترتيب وتوصيف كل مجموعة منها فى طائفة تتحد فى مميزاتها وخصائصها عن نظيراتها من المجموعات الأخرى، وتستقل بذاتها مكونة مجموعة من الجرائم المتميزة – استرشاداً فى ذلك بتقسيم قانون العقوبات للجنايات والجنح المضرة بالمصلحة العمومية (الكتاب الثانى)، الى جرائم مضرة بأمن الحكومة من جهة الخارج (م ٧٧ – م ٨٥ «أ»)، وجرائم مضرة بأمن الحكومة من جهة الداخل (م ٨٦ – م ١٠٥)، جرائم المفرقعات (م ١٠٢ «أ» – م ١٠٢ «و»)، جرائم الرشوة (م ١٠٣ – م ١١١) واختلاس المال العام والعدوان عليه والغدر (م ١١٢ – م ١١٩) ...، وكذلك تقسيمه للجنايات والجنح التى تحصل لآحاد الناس (الكتاب الثالث)، إلى جرائم القتل والجرح والضرب (م ٢٣٠ – م ٢٥١ «م»)، وجرائم الحريق عمداً (م ٢٥٢ – م ٢٥٩)، وجرائم هتك العرض وإفساد الاخلاق (م ٢٦٧ – م ٢٧٩)، وجرائم السرقة والاغتصاب (م ٣١١ – م ٣٢٧) ...

• أهمية تقسيم الجرائم المعلوماتية:

يبرز أمر تقسيم الجريمة المعلوماتية باعتباره أمراً غير نظرياً، حيث أنه ذو انعكاسات عملية متعددة تترتب عليه، يمكن إجمالها فيما يلى[1]:

- المساعدة على تحديد مدى الخطورة الإجرامية لمقترفى الأفعال غير المشروعة لجرائم المعلوماتية، وبالتالى وضع آلية فعالة للعقاب.
- تحديد مدى الأضرار الناجمة عن كل طائفة من تلك الطوائف، وتحديد أكثرها ضرراً على الإطلاق بحيث يمكن توجيه المكافحة إليها أولاً، على اعتبار أنه يصعب مواجهة كافة جرائم المعلوماتية فى ذات الوقت.
- تصنيف وتقسيم – جرائم المعلوماتية يكون مفيداً فى مسألة كيفية المواجهة داخل حدود الدولة الواحدة، وأنه يكون مفيداً كذلك بالنسبة لتحديد درجة التعاون الدولى المطلوب، للمساعدة فى كشف وتعقب تلك النوعية من الجرائم.
- يساعد على وضع تصور عام فى المعاونة الفنية، للكشف عن الأفعال غير المشروعة المرتبطة بالمعلوماتية وأجهزة الحاسب، لتعقبها وللتحقيق والمحاكمة بشأنها، إذ تختلف جرائم المعلوماتية من حيث النظر إلى البساطة أو الصفة المركبة فى ارتكابها أو إحداث أثرها وترتيب نتائجها.
- يساعد فى تحديد القواعد الخاصة بتنظيم تجريم الأفعال غير المشروعة المرتبطة بالمعلوماتية، وذلك إذا ما أمكن تصور الوصول إلى اتفاق دولى بشأن وضع قواعد دولية للتجريم.

وبصفة عامة فإن تقسيم الجريمة المعلوماتية هو الذى يرسى قواعد إدراج أى فعل من الأفعال الإجرامية المستحدثة – والمرتبط ارتكابها ارتباطاً وثيق الصلة بالمعلوماتية وأنظمة الحاسوب – فى إحدى الطوائف الخاصة لجرائم

---

(١) د/ محمود محمد عبد النبى – جرائم الحاسب الآلى (الجزء الثانى) – مجلة الأمن العام – العدد ١٨٩ – السنة ٤٧ – أبريل ٢٠٠٥ – ص ٢٧.

المعلوماتية، وهو ما يعنى من ناحية أخرى سهولة تطبيق القواعد الثابتة والأسس القانونية فى الضبط والتفتيش والتحقيق والمحاكمة على تلك الجرائم المستحدثة غير المشروعة، مما يثمر خطوات أكثر فاعلية نحو تجنب الأضرار المترتبة عليها كلياً، أو تجنب زيادة ارتكابها على أقل تقدير، مما يعنى تفعيل دور الوقاية منها.

## المطلب الأول

## التقسيم الفقهي المقارن لجرائم المعلوماتية

تعددت الجهود الفقهية التى بذلت – على الصعيد الدولى أو الوطنى – من أجل وضع تقسيم يمكن الاعتماد عليه لجرائم المعلوماتية. وفى هذا المجال يبرز للمعلوماتية ثلاثة أدوار فى مضمار ارتكاب الجرائم، ودوراً رئيسياً فى مجال اكتشافها.

ففى مجال ارتكاب الجرائم المستحدثة يكون للنظام المعلوماتى الأدوار التالية، وهى:

**أ - المعلوماتية هدفاً للجريمة (Target of an offense)؛**

نظم المعلومات تكون هدفاً للجريمة، كما فى حالة الدخول غير المصرح به إلى النظام أو زراعة الفيروسات لتدمير المعطيات والملفات المخزنة أو تعديلها، وكما فى حالة الاستيلاء على البيانات المخزنة أو المنقولة عبر النظم المعلوماتية. ومن أوضح المظاهر لاعتبار نظم المعلومات هدفاً للجريمة فى مجال التصرفات غير القانونية عندما تكون السرية (Confidentiality) والتكاملية – السلامة – (Integrity) والقدرة أو التوفير (Availability) هى التى يتم ا لاعتداء عليها، بمعنى أن توجه هجمات الأختراق – النشاط الإجرامى – إلى المعلومات المخزنة بنظم المعلومات أو خدماته بقصد المساس بالسرية، أو المساس بالسلامة والمحتوى والتكاملية، أو تعطيل القدرة والكفاءة للأنظمة للقيام بأعمالها. وهدف هذا النمط الإجرامى هو نظام المعلوماتية وبشكل خاص المعلومات المخزنة

داخله بهدف السيطرة على النظام دون أن يكون له سلطة أو حق في ذلك، أو بدون أن يدفع المستخدم مقابل استخدامه (سرقة خدمات المعلوماتية، أو وقت النظم المعلوماتية)، أو المساس بسلامة المعلومات وتعطيل القدرة على تقديم خدمات نظم المعلومات(١).

وغالبية هذه الأفعال الإجرامية تتضمن ابتداء الدخول غير المصرح به إلى النظام الهدف (Unauthorized Access) والتي توصف بشكل شائع في هذه الأونة بأنشطة الهاكرز، كناية عن فعل الأختراق (Hacking).

والأفعال التي تتضمن سرقة المعلومات تتخذ أشكال عديدة معتمدة على الطبيعة التقنية للنظام محل الاعتداء، وكذلك على الوسيلة التقنية المتبعة لتحقيق الاعتداء، فالنظام المعلوماتي مخزن للمعلومات الحساسة كالملفات المتعلقة بالحالة الجنائية والمعلومات العسكرية وخطط التسويق... وغيرها. وهذه تمثل هدفاً للاعتداء عليها من العديد من الجهات بما فيها أيضاً جهات التحقيق الجنائي والأجهزة الأمنية والاستخبارية، ومن جانب أخر المنظمات الأرهابية والتكتلات الإجرامية، ولا يتوقف نشاط الاختراق على الملفات والأنظمة غير الحكومية، بل يمتد إلى الأنظمة الخاصة التي تتضمن بيانات معلوماتية قيمة(*).

---

(١) أيمن عبد الله فكري – جرائم نظم المعلومات – رسالة مقدمة للحصول على درجة الدكتوراه – كلية الحقوق – جامعة المنصورة – ٢٠٠٥/٢٠٠٦ – ص ٨٥.

(*) على سبيل المثال قد يتوصل أحد القراصنة للدخول إلى النظام المعلوماتي للحجز في أحد الفنادق لسرقة أرقام بطاقات الائتمان للنزلاء، كما تتضمن بعض طوائف هذا النمط الذي يستهدف المعلوماتية، أنشطة سرقة واعتداء على الملكية الفكرية كسرقة الأسرار التجارية، وإعادة إنتاج ونسخ المصنفات المحمية وتحديداً برامج الحاسب.

وفي حالات أخرى فإن أفعال الأختراق التي تستهدف أنظمة المعلومات الخاصة تستهدف منافع تجارية، أو إرضاء أطماع شخصية. (يراجع: د/ يونس عرب – جرائم الكمبيوتر والأنترنت – المعنى والخصائص والصور واستراتيجية المواجهة القانونية. (www. arablaw. .Org/Download/cyber crimes - General. doc.

**ب- المعلوماتية أداة لارتكاب جرائم تقليدية(*):**

تكون كذلك كما فى حالة استغلال نظم المعلومات للاستيلاء على الأموال بإجراء تحويلات غير مشروعة أو استخدام التقنية فى عمليات التزييف والتزوير، أو استخدام التقنية فى الاستيلاء على أرقام بطاقات ائتمان وإعادة استخدامها والاستيلاء على الأموال بواسطة ذلك[1]. كما أن نظم المعلومات كوسيلة قد تستخدم فى جرائم القتل، كما فى الدخول إلى قواعد البيانات الصحية والعلاجية وتحويرها، أو تحوير عمل الأجهزة الطبية والمعملية عبر التلاعب ببرمجياتها، أو كما فى اتباع الوسائل الإلكترونية للتأثير على عمل برمجيات التحكم فى الطائرة أو السفينة بشكل يؤدى إلى تدميرها وقتل ركابها[2].

**جـ- المعلوماتية بيئة الجريمة:**

تكون المعلوماتية بيئة للنشاط الإجرامى، كما فى نموذج تخزين البرامج المقرصنة فيها، أو فى حالة استخدام نظم المعلومات لنشر المواد غير القانونية واستخدامها أداة تخزين أو اتصال لصفقات ترويج أنشطة غير مشروعة فى تجارة المخدرات أو الشبكات الاباحية أو غسل الأموال عبر الدول.

ويمكن للحاسب الآلى أن يلعب الأدوار الثلاثة مجتمعه، مثال ذلك أن يستخدم أحد محترفى نظم المعلومات (HACKER) جهاز الحاسوب للتوصل دون تصريح إلى نظام مزود خدمات انترنت (مثل نظام شركة أمريكا أون لاين)، ومن ثم يستخدم الدخول غير القانونى لتوزيع برنامج مخزن فى نظامه (نظام

---

(*) Atool in the commission of a traditional offense.

(١) أيمن عبدالله فكرى - المرجع السابق - ص ٨٦.

وللمزيد يراجع: اللواء/ نجاح محمد فوزى - وعى المواطن العربى تجاه جرائم الاحتيال (بطاقات الدفع الإلكترونى نموذجاً) - الرياض - جامعة نايف العربية للعلوم الأمنية - سنة ١٤٢٨ هـ - ٢٠٠٧م.

(٢) انظر فى أمثلة لتلك الوقائع. د/ هشام فريد رستم - مرجع سابق - ص ٥٦ وما بعدها.

المخترق)، فهو بذلك ارتكب فعلاً موجهاً نحو نظم المعلومات بوصفها هدفاً للدخول غير المصرح به، ثم استخدم نظم المعلومات لنشاط اجرامى تقليدى (عرض وتوزيع المصنفات المقرصنة)، واستخدام جهاز الحاسوب خاصته كبيئة أو مخزن للجريمة عندما قام بتوزيع برنامج مخزن فى نظامه(١).

**د - دور المعلوماتية في اكتشاف الجريمة:**

تستخدم نظم المعلومات على نطاق واسع فى التحقيق الاستدلالى لمعظم الجرائم، فضلاً عن أن جهات تنفيذ القانون تعتمد على النظم التقنية فى إدارة المهام من خلال بناء قواعد بيانات ضمن جهاز إدارة العدالة والتنفيذ القانونى.

ومع تزايد نطاق جرائم نظم المعلومات، واعتماد مرتكبيها علي وسائل التقنية المتجددة والمتطورة، فإنه أصبح لزاماً استخدام ذات الوسائل لمواجهة الجريمة المعلوماتية والكشف عنها، إن لم تكن المواجهة تتطلب وسائل اكثر تقنية تلعب فيها نظم المعلومات دوراً هاماً محورياً، يهدف إلى كشف جرائم المعلوماتية وتتبع مرتكبها، وفى مواجهة أكثر فاعلية واحترافية تكون الغاية إبطال أثر الهجمات التدميرية لمخترقى نظم المعلومات، وتحديداً هجمات نشر الفيروسات، وسرقة الخدمة وقرصنة البرمجيات.

وكما يمكن أن يعتمد تقسيم الجريمة المعلوماتية على حسب الدور الذى يلعبه جهاز الحاسوب فى الجريمة فمن الممكن أن يكون عاملاً مساعداً فى ارتكابها – أى يكون دوره مكملاً (ثانويا) – وهناك حالات أخرى يكون فيها دور الحاسوب هاماً وفعالاً فى ارتكابها، إذ بدونه لا يتصور أن ترتكب الجريمة فيكون دوره فيها رئيسياً، وتكون الجريمة المعلوماتية وفقاً لذلك هى: «كل نشاط إجرامى يؤدى فيه نظام الحاسب دوراً لإتمامه. على أن يكون هذا الدور على قدر من الأهمية». ولا يختلف الأمر سواء كان الحاسب الآلى أداة لإتمام الجريمة أو محلاً لها(٢).

---

(١) أيمن عبد الله فكرى – المرجع السابق – ص ٨٧.

(٢) د/ نائلة عادل فريد قورة – جرائم الحاسب الاقتصادية (دراسة نظرية تطبيقية) – دار النهضة العربية – القاهرة – سنة ٢٠٠٣/٢٠٠٤ – ص ٢٥ وما بعدها.

وفى هذا الصدد قام العديد من الفقهاء والباحثين بمحاولات متنوعة اجتهادية لتقسيم الجرائم المعلوماتية. نبدأ بعرض هذه الاجتهادات بالتقسيم المقارن للفقهين Martin Vasik , Ulrich Sieber. ثم نعرض لبعض الاجتهادات الوطنية بعد ذلك، وختاماً نعرض للجهود الأوروبية الدولية فى ذات الشأن.

**- التقسيم الفقهي المقارن(١):**

**• تقسيم Ulrich Sieber(*) لجرائم المعلوماتية:**

قسم Ulrich Sieber جرائم المعلوماتية إلى ثلاثة أقسام:

– جرائم الحاسب الآلى الاقتصادية.

– جرائم الحاسب الآلى التى تعتدى على الحياة الخاصة.

– جرائم الحاسب الآلى التى تهدد المصالح القومية أو السلامة الشخصية للأفراد(٢).

**أ - جرائم الحاسب الآلي الاقتصادية:**

تمثل هذه النوعية القسم الرئيسى لجرائم المعلوماتية، وقد أخرج من نطاقها الأفعال التى تضر بنظام الحاسوب، عن طريق الخطأ أو الأهمال ويندرج تحتها الجرائم التالية:

– الاحتيال المعلوماتى.

هو تلك الأفعال التى تقوم على التلاعب فى نظم المعلومات، للحصول بغير حق على أموال أو أصول أو خدمات.

---

(١) أيمن عبد الله فكرى – المرجع السابق – ص ٨٨ وما بعدها.

(*) محامى متخصص فى الكتابة فى مجال جرائم نظم المعلومات، وله مجموعة من المؤلفات بداية من سبعينيات القرن الماضى.. للمزيد فى ذلك يراجع: محمد سامى الشوا – بحث مترجم مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى – الفترة من ٢٥: ٢٨ أكتوبر ١٩٩٣ بعنوان جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات.

(2) Sieber ulrich: The international Emergence of criminal information Law, cral Heymanns verlag K.G., 1992, pp. 3-27.

- التجسس المعلوماتى (فى نطاق قطاع الأعمال).

تقوم تلك الجرائم على اختراق النظام المعلوماتى من أجل الاستفادة بما يتم التوصل إليه من معلومات.

- قرصنة برامج الحاسب الآلى.
- الإتلاف المعلوماتى. (سواء تعلق بالمكونات المادية أو غير المادية).
- الدخول غير المصرح به للنظام المعلوماتى.
- سرقة الخدمات أو الاستعمال غير المصرح به للنظام المعلوماتى.
- الجرائم التقليدية فى نطاق قطاع الأعمال، والتى يساعد النظام المعلوماتى فى ارتكابها.

**ب- الجرائم المتصلة بانتهاك حرمة الحياة الخاصة:**

مع الأهتمام بظاهرة الجريمة المعلوماتية، بدأ ظهور حماية الحياة الخاصة من الاعتداءات المعلوماتية، ويرجع سبب ذلك إلى ما أحدثته المعلوماتية فى مجال جمع وتخزين واستدعاء المعلومات من تطور كبير.

وقد تناول هذا القسم أربعة أشكال من تهديدات للحياة الخاصة، تمثلت فى الآتى:

- استخدام بيانات شخصية غير صحيحة.
- جمع وتخزين بيانات صحيحة ولكن على نحو غير مشروع.
- الإفشاء غير المشروع للبيانات الشخصية وإساءة استخدامها.
- مخالفة القواعد والإجراءات الشكلية فى نطاق القواعد التشريعية للخصوصية المعلوماتية.

**جـ- الجرائم التي تهدد المصالح القومية أو السلامة الشخصية للأفراد:**

نتيجة لتداخل نظم المعلومات فى مجالات الحياة المختلفة، لم تعد قاصرة

على الاعتداء على الحياة الخاصة أو الذمة المالية، وإنما امتدت لتشمل جانب أخر تتمثل خطورته على الأمن القومي للدولة وتهديد سلامة الأفراد، مثل(١):

- الاعتداء على أنظمة الدفاع في الدولة.
- الاعتداء على أنظمة الطيران، والتحكم الإلكتروني بما يؤثر على الأفراد وسلامتهم البدنية.

**- تقسيم Martin Vasik لجرائم المعلوماتية:**

قسم Vasik جرائم المعلوماتية إلى ثلاثة أقسام أساسية، يندرج تحت كل قسم مجموعة من الأفعال غير المشروعة، وقد راعى في هذا التقسيم التعرف على أنماط السلوك المختلفة التي تندرج تحت كل مسمى ومدى اتفاقها مع القواعد التي تحكم القانون الجنائي(٢). ويمكن استعراض تقسيم Vasik للجرائم المعلوماتية على النحو التالي:

أ - الدخول والاستعمال غير المصرح بهما للنظام المعلوماتي.

ويندرج تحت مسمى هذه الجريمة الأفعال الآتية:

- الدخول غير المصرح به للنظام المعلوماتي.
- الدخول غير المصرح به للنظام المعلوماتي بنية ارتكاب جريمة معلوماتية أخرى.
- الاعتراض غير المشروع للنظام المعلوماتي.
- الأفعال غير المشروعة المتصلة بالمعلومات الشخصية المعالجة آلياً.
- الاستعمال غير المصرح به للنظام المعلوماتي.

---

(1) Sieber ulrich, The international hand book on computer crimerelated economic crime and the infringements of privacy, John Viley a sons, 1986, pp. 26-27.

(2) Martin Vasik, Computer crime, Oxford unversity Press, 1991, p.41.
مشار إليه لدى: أيمن عبد الله فكري – المرجع السابق – هامش ٢ – ص ٨٩.

ب- الاحتيال المعلوماتي وسرقة المعلومات.

وتتضمن هذه الجريمة الأفعال الآتية:

- التلاعب في المعلومات المعالجة الكترونياً بقصد تحقيق ربح مادي غير مشروع.
- تزوير المعلومات المعالجة آلياً بنية استخدامها في أغراض غير مشروعة.
- الحصول غير المشروع على المعلومات المعالجة آلياً.
- قرصنة البرامج المعلوماتية.

جـ- الجرائم التي يساعد الحاسب الآلي على ارتكابها.

يندرج ضمن نطاق تلك الفئة من جرائم المعلوماتية، مجموعة الأفعال الآتية:

- التخريب والإتلاف سواء انصب على المكونات المادية أو غير المادية (المنطقية).
- الاستعمال غير المشروع للحاسبات، إعاقة المستخدمين الشرعيين للنظام المعلوماتي عن الوصول للمعلومات.
- استخدام نظم المعلومات للاعتداء على سلامة أمن الأفراد.
- التهديد بتدمير النظم المعلوماتية لابتزاز المجني عليهم.
- الإفشاء غير المشروع للمعلومات المؤتمن عليها بمقتضى الوظيفة.
- صناعة وبيع المعدات والأدوات التي تساعد على ارتكاب الجريمة.

## المطلب الثاني

## التقسيم الدولي للجريمة المعلوماتية

### أولاً: تقسيم المجلس الأوروبي للجريمة المعلوماتية:

نوقش موضوع ارتباط الكمبيوتر بالجريمة أول مرة عام ١٩٧٦م، وذلك في المؤتمر الثاني عشر لمديري معاهد البحوث في علم الإجرام تحت رعاية المجلس الأوروبي، وفي عام ١٩٨٣م أخذت هيئة التعاون الاقتصادي والتنمية (OECD)

على عاتقها دراسة إمكانيات التطبيقات والتوافقيات الدولية لقوانين الجريمة التى تحدد مشاكل جريمة الكمبيوتر (الجريمة المعلوماتية)(*)، وفى هذا الصدد فأن المجلس الأوربى قد استهل دراسته بخصوص الجرائم المرتبطة بالكمبيوتر برؤيته لتطوير خطوط الإرشاد لمساعدة المشرعين فى تحديد طبيعة الجريمة المعلوماتية والتى يتبغى تجريمها قانوناً، وقد تبنى مجلس الوزارة لمجلس الشورى الأوربى عدة توصيات لجرائم الكمبيوتر فى سبتمبر ١٩٨٩م(**).

---

(*) بدأ اهتمام منظمة (OECD) بالمشكلات التى آثارها ظهورا لنظم المعلوماتية فى الحياة الاقتصادية منذ عام ١٩٧٧م، وقد بدأ هذا الاهتمام فى بادئ الأمر يتجه إلى حماية الخصوصية من التهديد المعلوماتى لها، وأنتج هذا الاهتمام قواعد إرشادية وتوصيات للدول الأعضاء فى تشريعاتها الوطنية، ونصت على عقوبة جنائية فى حالة مخالفة تلك القواعد الارشادية والتوصيات، والتى تمثلت فيما يتعلق بحماية البيانات ذات الطبيعة الشخصية، وهذه القواعد والتوصيات هى:

- تحديد الغرض الذى يتم تجميع البيانات من أجله.
- مراعاة القواعد الشكلية الخاصة بالمحافظة على البيانات.
- الانفتاح، ومقتضى ذلك أن يكون ما يتعلق بالحياة الشخصية من سياسة عامة للتطوير والتخطيط والتطبيق معلنة للكافة لمعرفتها.
- المشاركة الفردية، ومقتضاها أن يكون للأشخاص الحق فى الوصول والتعرف على البيانات الخاصة بهم، وحقهم فى الرد عليها والتعديل فيها.
- حدود الاستخدام يعنى ان يكون استخدام البيانات فى الغرض المحدد للجهة، ولا يتم الخروج على ذلك إلا بموافقة الشخص.
- المساءلة أو المحاسبة. يعنى مساءلة الشخص المنوط به التعامل مع البيانات ذات الطبيعة الشخصية، عن مدى كفالته للقواعد والمبادئ السابقة عند تعامله مع تلك البيانات.

يراجع فى ذلك:

- O.E.C.D. Guidelines on the protection of privacy and transborder flows of Personal data. 1980.
- O.E.C.D Transborder data flows Anoverview of issue, Report Dsti/ Iccp/83, 29, 11 October, 1983, Dhouwer, privacy and transborder data flows, vrije university it, Breessels, 1984, pp. 9 et seq.

(**) قامت اللجنة الأوروبية المشكلة لدراسة مشاكل الجريمة من عام ١٩٨٥ حتى ١٩٨٩ بتقديم تقرير رفعته إلى لجنة الخبراء، التى قدمته بدورها للجنة الوزراء فى عام ١٩٨٩، والذى أصدر

=/=

وقبل ذلك نوقش موضوع منع الجريمة المرتبطة بالكمبيوتر فى تقرير تحت عنوان (اقتراحات المواجهة الدولية تجاه صور تطور الجريمة) والذى تم تحضيره بواسطة الأمم المتحدة فى عام ١٩٨٧م، وفى ختام الاجتماع الثانى عشر لمجلس نواب الأمم المتحدة الثامن لمنع الجريمة والذى عقد عام ١٩٩٠م، تم مناقشة مشروع لحلول مشكلة الجريمة المرتبطة بالكمبيوتر، مع الأخذ فى الاعتبار أهمية تركيز جهود الدول الأعضاء لضبط هذه الجرائم المعلوماتية للأضرار الجسيمة التى تخلفها.

---

- التوصية رقم ٨٩ (٩)، والتى تضمنت الإرشادات الموجهة إلى المشرعين فى الدول الأعضاء، بالنص لديهم على مكافحة الجريمة المعلوماتية، وذلك من خلال إدراج طائفتين من التجريم الأولى تضم القائمة الاساسية، والثانية تضم مجموعة من الأفعال الاختيارية.

- وتشمل الطائفة الأولى الإلزامية الأفعال التالية:
  - الاحتيال المعلوماتى.
  - التزوير المعلوماتى.
  - الإتلاف المعلوماتى.
  - الاعتراض غير المصرح به لنظام الحاسب.
  - إعاقة النظام المعلوماتى عن وظيفته.
  - الدخول غير المشروع للنظام المعلوماتى.
  - النسخ غير المشروع لبرامج الحاسب.
  - النسخ غير المشروع للتصميمات الخاصة بدقائق الحاسبات الآلية.
- بينما تضمنت القائمة الاختيارية من الأفعال المجرمة ما يلى:
  - التعديل فى البيانات المخزنة بالحاسب أو ببرامجه وذلك فى الحالات التى لا يؤدى فيها هذا التعديل إلى إتلافها (سواء بالنسبة للبيانات أو البرامج).
  - التجسس المعلوماتى.
  - الاستعمال غير المصرح به لنظام الحاسب الآلى.
  - الاستعمال غير المصرح به لبرامج الحاسب الآلى التى تشملها الحماية القانونية.

يراجع فى ذلك:

- Les Recommandation du congrés de L'A.F.D.P Section II infraction information autres crimes contre la technologie informatique R.T.D.P. p. 1995. Vol. 66. pp. 2 ets.

وفى ١١ سبتمبر سنة ١٩٩٥م عقد مؤتمر وزراء الدول الأعضاء فى المجلس الأوروبى بخصوص بحث مشاكل قانون الإجراءات الجنائية المتعلقة بتكنولوجيا المعلومات، وقد أخذت توصية اللجنة لهذا المؤتمر بتسمية المرحلة التى يعيش فيها العالم حالياً بمرحلة المجتمع المعلوماتى، حيث ورد فى صدد هذه التوصية:

(... إن التطور فى نظم المعلومات الاليكترونية سوف يُعجل بتحول المجتمع التقليدى إلى مجتمع معلوماتى، من خلال إيجاد فضاء جديد لكل أنواع الاتصالات والعلاقات...)(*).

ومع زيادة حركات التمرد والخروج على الثوابت والتى قد بدأت فى مجالات الأدب والفن والعمارة، فأنها سرعان ما امتدت إلى مجالات أخرى متعددة منها مجال تكنولوجيا الاتصالات والمعلومات، وقد أدى هذا التمرد إلى تنوع الجرائم المعلوماتية وانتشارها، وذلك ما بين أعمال قرصنه وتوفير مواقع إباحية، ثم تطوير الأمر بصورة غير متصورة مع ظهور مجموعات تطلق على نفسها (مجموعات الكراهية على الإنترنت Hate Groups on the internet)، تلك المجموعات التى تزدرى بكل القيم الدينية والأخلاقية والاجتماعية السائدة فى المجتمعات، وبصفة خاصة تلك المرتبطة بالأسرة، كذلك مواقع الإلحاد التى تطالب بإلغاء الدين والدولة والأسرة وتحرير الإنسان من تلك الأصفاد(١).

على أن الانفلات الذى شمل شتى مناحى الحياة، بما فيها الإنفلات الدينى والأخلاقى والاجتماعى والاقتصادى والسياسى، قد يعطى تفسيراً مقنعاً لحالة النمو المتزايد والمطرد للجرائم الكونية أو المعلوماتية، ولذلك ومن أجل هذه

---

(*) تسمية المجتمع المعلوماتى التى أطلقها آلفين توفلر هى التسمية التى أخذت بها توصية لجنة وزراء الدول الأعضاء فى المجلس الأوروبى المنعقد فى ١١ سبتمبر سنة ١٩٩٥م. (د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والاجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست...) – مرجع سابق – ص ١١).

(١) د/ هلالى عبد اللاه أحمد – المرجع نفسه – ص ٢٥.

النوعية من الجرائم حرص المجلس الأوروبي على صياغة اتفاقية لمكافحة الجرائم المعلوماتية والتغلب عليها، كما حرصت بعض الدول على أن تضمن تشريعاتها هذه النوعية من الجرائم. إما عن طريق النص عليها استقلالاً فى تشريعات مستقلة(*)، وإما عن طريق تحديث قوانيها وإدماجها فى هذه القوانين(**).

وقد تجلى حرص المجلس الأوروبى على التصدى للاستخدام غير المشروع للحاسبات الآلية وشبكات المعلومات، فى اتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١ المتعلقة بالإجرام الكونى، (الجريمة الافتراضية).

**ثانياً: التقسيم الفرنسي للجريمة المعلوماتية:**

قسم المشرع الفرنسى فى القانون رقم ٨٨/١٩ جرائم الاعتداء على معطيات النظام الآلى لمعالجة البيانات إلى عدة جرائم تمثلت فى تقسيم الحماية بالنظر إلى النظام المعلوماتى.. والمعلومات. وبيان هذه الجرائم(١):

- الدخول أو البقاء غير المصرح به لنظام معالجة آلية البيانات أو فى جزء منه.
- الإتلاف المعلوماتى لمحتوى النظام الألى لمعالجة البيانات.
- إعاقة أو إفساد نظام المعالجة الآلية للبيانات.
- التزوير فى وثيقة مبرمجة.

---

(*) مثال ذلك قانون أساءة استخدام الحاسب فى المملكة المتحدة الصادر فى ٢٩ يونيو سنة ١٩٩٠م، والذى طبق اعتباراً من ٢٩ أغسطس سنة ١٩٩١م.

(**) ومن أبرز هذه النوعية من التشريعات قانون العقوبات الفرنسى الجديد الصادر سنة ١٩٩٢ والمعمول به منذ أول مارس سنة ١٩٩٤م، والذى أضاف فصلاً ثالثاً للباب الثانى من القسم الثالث من قانون العقوبات تحت عنوان: (انتهاكات نظم المعالجة الآلية للبيانات) ويتكون هذا الفصل من المواد ١/٣٢٣ إلى ٧/٣٢٣.

(١) ايمن عبد الله فكرى – مرجع سابق – ص ٩٦.

- استخدام وثيقة مبرمجة مزورة.
- المعاقبة على الشروع في الجرائم السابقة.
- المعاقبة على المساهمة الجنائية في الجرائم السابقة.

وقد اتخذ قانون العقوبات الفرنسي الحديث (بالنسبة لجرائم المعلوماتية) ذات النهج الوارد في القانون رقم ١٩/٨٨، مع قيام المشرع بحذف المادة ٤٦٢-٥، ٦ الخاصة بالتزوير في وثيقة مبرمجة واستخدامها، حيث اتخذ منهج موسع لمفهوم التزوير ومحله بالمادة ٤٤١-١، وهو الأمر الذى يكون المشرع الفرنسي أراد به أن يدخل التزوير المعلوماتي ضمن نطاق التزوير التقليدى[1].

**ثالثاً: تقسيم الجرائم المعلوماتية في ضوء الاتفاقيات الدولية:**

في ظل هذا الحراك الأوروبي والدولي لوضع تشريع جنائي ينال من الأفعال التي طالت النشاط المعلوماتي، وجنحت بالفكر المستحدث للمعلوماتية من فائدة للبشرية إلى أفعال إجرامية يصعب تتبعها، أفرزت جرائم منظمة تهدد الكيان الإنساني، نجد أن المشرع المصرى قد قصر حمايته الجنائية للنظام المعلوماتي على مجالين من مجالات الحاسب الآلى[2]:

- **أولهما:** البرامج وقواعد البيانات وهذه اعتبرها ضمن المصنفات المشمولة بحق المؤلف[3].
- **وثانيهما:** البيانات الفردية التي تقتضي إجراء إحصاء للسكان، وكذلك البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين[4]. وقد نص على العقوبات التي ينبغي تطبيقها في حالة الاعتداء على هذه البيانات.

---

(1) Deveze (J), Atteintes aux systémes de traitement automatise de données, J.C.P, Ed, 1998.

(٢) د/ هلالى عبد اللاه أحمد - تفتيش نظم الحاسب الآلى - مرجع سابق - ص ١١١ وما بعدها.

(٣) القانون رقم ٣٨ لسنة ١٩٩٢م الخاص بتعديل بعض أحكام قانون حق المؤلف رقم ٣٥٤ لسنة ١٩٥٤، والمعدل بالقانون رقم ٢٩ لسنة ١٩٩٤م (نشر بالجريدة الرسمية العدد ١٦ (تابع) الصادر في ٢١ ابريل سنة ١٩٩٤م).

(٤) القانون رقم ١٤٣ لسنة ١٩٩٤ في شأن الأحوال المدنية الصادر في ٩ يونيه ١٩٩٤م (نشر بالجريدة الرسمية العدد ٢٣ تابع الصادر في ٩ يونيه ١٩٩٤).

أما بقية الجرائم المعلوماتية - سواء كان الحاسب الآلي موضوعاً للجريمة أو أداة لارتكابها - فلا تشملها الحماية الجنائية.

وإزاء هذا الفراغ التشريعي، لم يقف الفقهاء مكتوفي الأيدي، بل حاول البعض بسط سلطان النماذج التشريعية التقليدية المعروفة بحيث تغطي هذه النوعية الجديدة من الجرائم(*). ورغم وجاهة هذه الاجتهادات الفقهية ألا أنها تصطدم بمبدأ الشرعية الجنائية ومنهج تفسير قانون العقوبات، وما يتطلبه من عدم جواز القياس في نصوص التجريم والعقاب، الأمر الذي يقتضي تدخل المشرع الجنائي لمواجهة هذه الصور الإجرامية المستحدثة وسد هذا النقص التشريعي، جاعلاً قبلته في ذلك صوب الاتفاقيات الدولية للمعلوماتية.

وفي هذا الخصوص فإن المؤتمر الدولي الخامس للجمعية الدولية لقانون العقوبات - والذي عقد في ريو دي جانيرو بالبرازيل في الفترة من ٤:٩ سبتمبر سنة ١٩٩٤م - جاء ضمن توصياته قائمة تشمل الحد الأدنى من الأفعال - المستهدفه - للنظم المعلوماتية - التي أوصى المجلس الأوروبي Le conseil dé L'Eurape بتجريمها إذا حدثت عمداً، من الممكن أن يسترشد بها المشرع المصري لمواجهة الجرائم الحديثة للمعلوماتية: وهذه الأفعال كما يلي:

١- **الغش المرتبط بالحاسب الآلي Le fraude relative à Lo'rdinateur**، ويشمل الإدخال L'insertian، الإتلاف L'Altération، المحو L'effacement أو الطمس La Suppression، لبيانات أو برامج الحاسب الآلي أو أي عوائق أخرى، تؤثر في مجرى معالجة البيانات، وتتسبب في ضياع

---

(*) من أمثلة الاجتهادات وللمزيد من المعرفة يراجع: د/ جميل عبد الباقي الصغير - القانون الجنائي والتكنولوجيا الحديثة - الكتاب الأول (الجرائم الناشئة عن استخدام الحاسب) - القاهرة - دار النهضة العربية - الطبعة الأولى - سنة ١٩٩٢م، د/ هدى حامد قشقوش - جرائم الحاسب الألكتروني - مرجع سابق - د/ محمد سامي الشوا - ثورة المعلومات وانعكاسها على قانون العقوبات - القاهرة - دار النهضة العربية - سنة ١٩٩٤. وأيضاً انظر ما يلي في الدراسة.. ص٢٣٩.

ملكية الشخص، أو إحداث خسارة اقتصادية له، أو فقدان الحيازة وذلك بقصد حصول الفاعل على نفع اقتصادى غير مشروع له أو لغيره.

٢- **التزوير المعلوماتي La falrification informatique**: ويضم الإدخال، الإتلاف، المحو، أو الطمس لبيانات أو برامج الحاسب، أو أى عوائق أخرى تؤثر فى مجرى معالجة البيانات ترتكب بهذه الطريقة أو فى مثل تلك الحالات، ويكون منصوصاً عليها فى التشريع الوطنى بوصفها جريمة تزوير لو كانت قد ارتكبت بخصوص موضوع تقليدى لمثل هذه الجريمة.

٣- **الأضرار ببيانات وبرامج المعلوماتية**: ويشمل المحو، الإتلاف، التعطيل La dél-ériaratio، أو الطمس غير المشروع لبيانات وبرامج المعلوماتية، أو إخفاء البيانات أو البرامج بدون وجه حق.

٤- **تخريب الحاسبات Le Sabotage d'ardinateurs**: ويضم الإدخال، الإتلاف، المحو، أو الطمس لبيانات وبرامج الحاسب، أو أى عائق آخر للنظم المعلوماتية، بنية تعطيل أو أعاقة أو تشويش أو منع وظيفة الحاسب أو نظام الاتصالات.

٥- **الولوج غير المصرح به(*) L'accés nan autorisée**: وهو الولوج غير المشروع لنظام معلوماتى أو مجموعة نظم، عن طريق انتهاك الإجراءات الأمنية.

٦- **الاعتراض غير المصرح به L'interception nan autorisée**: وهو اعتراض بدون وجه حق، يتم عن طريق وسائل فنية للاتصال، تتجه نحو نظام معلوماتى أو عدة نظم أو شبكة اتصالات، حيث تعمل من خلال تواجدها داخل هذا النظام المعلوماتى أو مجموعة النظم الشبكية.

---

(*) هو الإدخال بدون وجه حق لنظام كمبيوتر أو شبكة، عن طريق اختراق معايير الحماية الخاصة بها.

• كذلك توجد قائمة أخرى للمجلس الأوروبى يطلق عليها القائمة الاختيارية Optionnelle، تحدد أيضاً الخطوط الإرشادية بالنسبة للأفعال التكميلية التى يمكن تجريمها إذا ارتكبت عن طريق العمد، وهى:

• إتلاف بيانات أو برامج المعلوماتية، وهو الإتلاف غير المشروع لبيانات أو برامج المعلوماتية.

• التجسس المعلوماتي L'espionnage informatique، ويندرج تحته الاقتناء L'aquisition عن طريق وسائل غير مشروعة، أو الإفشاء La révélation، أو النقل Le transfert، أو الاستعمال بدون وجه حق أو مبرر قانونى لسر اقتصادى أو تجارى، بقصد إحداث ضرر اقتصادى بحائز السر، أو بقصد الحصول على مزية اقتصادية غير مشروعة، سواء كانت للشخص ذاته أو لشخص آخر.

• استنساخ نموذج بدون تفويض: وهو استنساخ نموذج محمى بالقانون وبدون وجه حق لمنتج شبه موصل، أو الاستغلال التجارى أو الاستيراد بهدف الاستنساخ بدون تصريح للنموذج أو لمنتج شبه موصل يصنع باستخدام النموذج.

ومن أحدث الاتفاقات الدولية التى تصدت للاستخدام غير المشروع للحاسبات وشبكات المعلومات، اتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١، وتبين المذكرة التفسيرية(*) أن الهدف من القسم الأول من الباب الثانى من

---

(*) راجع باللغة الفرنسية المذكرة التفسيرية لاتفاقية بودابست ٨ نوفمبر ٢٠٠١.

- "Convenation sur la cybercriminalite" STE No. 185, Rapport explicatif, adopté le 8 Novermbre 2001, p. 10 ets.

وراجع باللغة الانجليزية مسودة المذكرة التفسيرية لاتفاقية بودابست ستراسبورج ١٤ فبراير سنة ٢٠٠١.

- "Draft Explanatory memorandum to the Draft convention on cyber-crime" Strasbourg. 14 February 2001.

الاتفاقية بمواده من ٢-١٣ هو تحسين أو اصلاح وسائل منع وقمع الإجرام المعلوماتي Améliorer les moyens de prévenir et de réprimer la criminli-té informatique وذلك من خلال تحديد معيار بالحد الأدنى المشترك الذى يسمح باعتبار بعض التصرفات من قبيل الجرائم الجنائية، وهذا النوع من التجانس Une harmonisation يسهل مكافحة هذه النوعية من الجرائم على المستويين القومى والدولى، كما أن التوافق La concordance بين التشريعات الداخلية يمكن أن يقاوم التصرفات غير المشروعة التى يتم ارتكابها، وبالأحرى لدى الطرف الذى كان يطبق من قبل معياراً أقل صرامة(١).

وتشير المذكرة التفسيرية إلى أن قائمة الجرائم المدرجة فى هذا القسم تمثل الحد الأدنى للتوافق Un consensus minimal الذى لا يستعبد أن يتم استكمال هذه القائمة فى القانون الداخلى، وأن هذه القائمة تستند إلى درجة كبيرة على المبادئ الواردة فى التوصية La Recommandation رقم ٩ لسنة ١٩٨٩ للمجلس الأوربى بخصوص الجرائم المتعلقة بالحاسب، وكذلك أعمال المنظمات العالمية الأخرى سواء العامة أم الخاصة، كما أنها من ناحية أخرى تأخذ فى الاعتبار أيضاً الممارسات غير المشروعة Pratiques illictes الأكثر حداثة Plusrécentes والمرتبطة بالتوسع فى استخدام شبكات الاتصال عن بُعد(٢)(*).

---

(١) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية – مرجع سابق – ص ٥٥، ويراجع أيضاً: لواء د/ محمود وهيب السيد – مفاهيم أساسية فى أمن المعلومات – مجلة الأمن العام – العدد ١٨٣ – أكتوبر ٢٠٠٣ – ص ٢٧ وما بعدها.

(٢) د/ هلالى عبد اللاه أحمد – المرجع نفسه – ص ٥٥ وما بعدها.

(*) ويتفرع القسم الأول إلى خمسة عناوين Titres رئيسية هى:

**العنوان الأول Le Titre 1**: ويضم جوهر جرائم الحاسب أو الجرائم المعلوماتية Les in-fractions informatiques تلك الجرائم التى تعرف بالجرائم ضد سرية البيانات وسلامة البيانات والنظم، وهذه الجرائم تمثل التهديدات الرئيسية وفقاً للمناقشات التى دارت حول أمن الحاسبات والبيانات، والتى تؤثر على نظم المعالجة الآلية وارسال البيانات.

وتشمل العناوين من ٢-٤ على نوعية أخرى من جرائم الحاسب أو الجرائم المعلوماتية، وهى

-/-

وإذا كانت نصوص قانون العقوبات تنطبق على الجرائم المرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية قد حرصت عى إيضاح أن الاتفاقية تستخدم مصطلحات تكنولوجية محايدة Meutre بطريقة يمكن معها تطبيق جرائم قانون العقوبات على كل من التكنولوجيا الأتية والمستقبلة.

ومن النقاط الهامة التى ركزت عليها المذكرة التفسيرية أيضاً ضرورة أن يكون ارتكاب الجرائم المحصاة فى هذه الاتفاقية (دون حق)، ويتجلى ذلك فى نصها: (يشترط فى تجريم الأفعال المذكرة فى هذه الاتفاقية أن يكون القيام بالفعل دون حقSans Droit).

كذلك تقرر المذكرة التفسيرية أن كل الجرائم المدرجة فى هذه الاتفاقية يجب أن تكون مرتكبة بطريقة عمدية Facon intentionnelle، من أجل تقرير

---

-- التى تلعب دوراً أكبر فى الممارسة العملية، حيث يتم استخدام أجهزة الحاسب والاتصالات كوسيلة للهجوم على بعض المصالح القانونية Certains intérést Juridiques، والتى كقاعدة عامة يحميها مسبقاً قانون العقوبات من هذه الهجمات عن طريق استخدام الوسائل التقليدية à L'aide de moyens classiques.

العنوان الثانى Le Titre 2: وقد تم إضافة جرائم هذا العنوان وهى الغش المعلوماتى Le Fraude informatique والتزوير المعلوماتى La Falsification informatique، من خلال الاقتراحات التالية لتوصية المجلس الأوربى رقم ٩ لسنة ١٩٨٩.

العنوان الثالث Le Titre 3: ويغطى الجرائم المرتبطة بالمحتوى Les infractions se rapportat ou contenu، بمعنى الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية، والذى يمثل أحد نماذج تنفيذ الجريمة الأكثر خطورة، والذى بدأ فى الظهور حديثاً.

العنوان الرابع Le Titre 4: يحدد الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها Les infractions liées aux atteintes à La propriété intellectulle et aux drouts connexes وقد نصت الاتفاقية على هذه النوعية من الجرائم، وذلك لأن الانتهاكات الواقعة على الملكية الفكرية هى أحد اشكال الإجرام المعلوماتى الأكثر شيوعاً، والذى بازدياد نسبته يزداد قلق وانشغال العالم بأسره.

العنوان الخامس Le Titre 5: يشتمل على أحكام أضافية بخصوص الشروع La tenta-tive والاشتراك Complicité، وأيضاً الجزاءات والاجراءات أو التدابير، وذلك طبقاً للمعايير الدولية الحديثة بالنسبة لمسئولية الأشخاص المعنوية.

المسئولية الجنائية وفى بعض الحالات يتطلب الأمر عنصراً عمدياً خاصاً، أو بتعبير آخر قصد خاص لاستكمال عناصر الجريمة، مع ترك المعنى الدقيق لكلمة عمداً أو قصداً للقوانين الداخلية.

**رابعاً: التقسيم الأمريكي لجرائم المعلوماتية:**

يعد هذا التقسيم الأكثر شيوعاً فى الدراسات والأبحاث الأمريكية، مع وجود فروق بينها من حيث مشتملات التقسيم ومدى انضباطه. كما أن هذا التقسيم يعد المعيار المعتمد لتقسيم جرائم المعلوماتية فى مشروعات القوانين النموذجية التى وضعت من جهات بحثية، بقصد محاولة إيجاد الانسجام بين قوانين الولايات المتحدة المتصلة بهذا الموضوع، ويعكس هذا الاتجاه التقسيم الذى تضمنه مشروع القانون النموذجى لجرائم نظم المعلومات الموضوع عام ١٩٩٩م الذى تم وضعه بمعرفة فريق بحثى أكاديمى، والمسمى Model state computer crimes code[1]، وفى نطاقه تم تقسيم جرائم نظم المعلومات إلى:

- الجرائم الواقعة على الأشخاص.
- الجرائم الواقعة على الأموال (عدا السرقة).
- جرائم السرقة والاحتيال والتزوير.
- الجرائم ضد الآداب (عدا الجرائم الجنسية).
- الجرائم ضد المصالح الحكومية.

ويلاحظ أن المشاركة تقوم على فكرة الغرض النهائى (المحل النهائى) الذى يستهدفه الاعتداء، لكنه ليس تقسيم منضبطاً ولا هو تقسيم محدد الأطراف، فالجرائم التى تستهدف الأموال تضم من حيث مفهومها السرقة والاحتيال، أما الجرائم التى تستهدف التزوير فتمس الثقة والاعتبار، والجرائم الواقعة ضد الآداب قد تتصل بالشخص وقد تتصل بالنظام والأخلاق العامة[2].

---

(1) http: // cybercrimes. net / 99MS CCC/ 99 MS CCC Main-html.

(١) ايمن عبد الله فكرى – مرجع سابق – ص ٩٦ وما بعدها.

وعلى كافة الأوجه فإنه تبعاً لهذا الفكر التشريعى، تنقسم الجرائم تبعاً لمساسها بالأشخاص والأموال على البيان التالى عرضه: -

**أولاً: الجرائم التي تستهدف الأشخاص:**

وتضم طائفتين رئيسيتين هما:

١- طائفة الجرائم غير الجنسية التى تستهدف الأشخاص(*).

Non - Sexual Crimes against Persons.

٢- طائفة الجرائم الجنسية (Sexual Crames)(**).

---

(*) تشمل القتل بالكمبيوتر Computer Murder، جرائم الإهمال المرتبط بالكمبيوتر Negligent Computer Homicide، والتحريض على الانتحار Soliciting or Encouraging Suicide، والتحريض القصدى للقتل عبر الإنترنت Intentional Internet Homicide Solicitation والتحرش والمضايقة عبر وسائل الاتصال الحاسوبى Harassment via Computerized Communication والتهديد عبر وسائل الاتصال الحاسوبى Intimidation via Computerized Communication والإحداث المتعمد للضرر العاطفى أو المشاركة بضرر عاطفى عبر وسائل التقنية Malicious Infliction of Emotional Distress utilizing Computere Communication و Reckless Infliction of Emotional Distress utilizing Computer Communication والملاحقة عبر الوسائل التقنية Chasing وأنشطة اختلاس النظر أو الإطلاع على البيانات الشخصية Online Voyeurism and Online Voyeurism disclosure وقنابل البريد الإلكترونى E-mail Bombing وأنشطة ضخ البريد الإلكترونى غير المطلوب أو غير المرغوب به Spamming utilizing Computerized Communication وبث المعلومات المضللة أو الزائفة Transmission of False Statements والانتهاك الشخصى لحرمة كمبيوتر (الدخول غير المصرح به) Personal trespass by computer.

(**) تشمل حض وتحريض القاصرين على أنشطة جنسية غير مشروعة Soliciting a Minor with a Computer for Unlawful Sexual Purposes وإفساد القاصرين بأنشطة جنسية عبر الوسائل الإلكترونية Corrupting a Minor with the use of a Computer for Unlawful Sexual Purposes وإغواء أو محاولة إغواء القاصرين لارتكاب أنشطة جنسية غير مشروعة Luring or Attempted Luring of a Minor by Computer for Unlawful Sexual Purposes وتلقى أو نشر المعلومات عن القاصرين عبر الكمبيوتر من أجل أنشطة جنسية غير مشروعة Receiving of Disseminating Information about a

-/-

ثانياً: جرائم الأموال المتضمنة أنشطة الاختراق والإتلاف(*).

Property Damage crimes Involving Intrusions.

---

-- والتحرش الجنسي بالقاصرين Minor by Computer for Unlawful Sexual Puposes Sexually Harassing a minor by use of a Comput- عبر الكمبيوتر والوسائل التقنية er for Unlawful Sexual Purposes ونشر وتسهيل نشر واستضافة المواد الفاحشة عبر الإنترنت بوجه عام وللقاصرين تحديداً Posting Obscene Material on the Internet و Trafficking In و Posting Or Receiving Obscene Material On The Internet و Obscene Material On The Internet Sending Obscene Material To Minors Over The Internet ونشر الفحش والمساس بالحياء (هتك العرض بالنظر) عبر الإنترنت Indecent Exposure On The Internet وتصوير أو إظهار القاصرين ضمن أنشطة جنسية Depicting Minors Engaged In Sexually Explicit Conduct- واستخدام الإنترنت لترويج الدعارة Pandering Obscenity Involving A Minor بصورة قسرية أو للإغواء أو لنشر المواد الفاحشة التي تستهدف استغلال عوامل الضعف والانحراف لدى المستخدم Using the Internet for Compelling Prostitution و Using the Internet for Pimping و Using the Internet for Promoting Prostiution والحصول على الصور والهاويات بطريقة غير مشروعة لاستغلالها في أنشطة جنسية Unauthorized Appropriation of Identity, Image, or Likeness for Unlawful Sexual Purposes وبإمعان النظر في هذا الأوصاف نجد أنها تجتمع جميعاً تحت صورة واحدة هي استغلال الإنترنت والكمبيوتر لترويج الدعارة أو إثارة الفحش واستغلال الأطفال والقصر في أنشطة جنسية غير مشروعة.

(*) تشمل أنشطة اقتحام أو الدخول غير المصرح به مع نظام الكمبيوتر أو الشبكة أما مجرداً أو لجهة ارتكاب فعل آخر ضد البيانات والبرامج والمخرجات Aggravated Computer Trespass و Computer Trespass و Disorderly Persons Offense وتخريب المعطيات والنظم والممتلكات ضمن مفهوم تخريب الكمبيوتر Computer Vandalism وإيذاء الكمبيوتر Computer Mischief واغتصاب الملكية Extortion وإنشاء البرمجيات الخبيثة والضارة Creation of Harmful Programs ونقلها عبر النظم والشبكات Transmission of Harmful Programs واستخدام اسم النطاق أو العلامة التجارية أو اسم الغير دون ترخيص Cyber Squatting وإدخال معطيات خاطئة أو مزورة إلى نظام كمبيوتر Introducing False Information Into a Computer or Computer System والتعديلات غير المصرح بها لأجهزة ومعدات الكمبيوتر Unlawful Modification of Computer Equipment or Supplies والإتلاف غير المصرح به لنظم الكمبيوتر (مهام نظم الكمبيوتر الوظيفية) Unlawful Modification of Computer Equipment or Supplies وأنشطة إنكار

-/-

**ثالثاً: جرائم الاحتيال والسرقةFraud and Theft crimes(*).**

**رابعاً: جرائم التزوير Forgery(**).**

**خامساً: جرائم المقامر والجرائم الأخري ضد الأخلاق والآداب(***).**

**G$ambling and other offenses Against Morality**

---

-- الخدمة أو تعطيل أو اعتراض عمل النظام أو الخدمات Unlawful Denial, Interruption, or Degradation of Access to Computer Unlawful Denial, Interruption, or Degradation of Access to Computer Services وأنشطة الاعتداء على الخصوصية Computer Invasion of Privacy (وهذه تخرج عن مفهوم الجرائم التى تستهدف الأموال لكنها تتصل بجرائم الاختراق) وإفشاء كلمة سر الغير-Disclosure of Another's Pass-word والحيازة غير المشروعة المعلومات Unauthorized Possession of Computer Information وإساءة استخدام المعلومات Misuse of Computer Information ونقل معلومات خاطئة Transmission of False Data.

(*) تشمل جرائم الاحتيال بالتلاعب بالمعطيات والنظم Fraud by Computer Manipulation واستخدام الكمبيوتر للحصول على أو استخدام البطاقات المالية للغير دون ترخيص Using a Computer to Fraudulently Obtain and use Credit Card Information أو تدميرها Damaging or Enhancing Another's Credit Rating والاختلاس عبر الكمبيوتر أو بواسطته Computer Embezzlement وسرقة معلومات الكمبيوتر Computer Information Theft وقرصنة البرامج Piracy Software وسرقة خدمات الكمبيوتر (وقت الكمبيوتر) Theft of Computer Services وسرقة أدوات التعريف والهوية عبر انتحال هذه الصفات أو المعلومات داخل الكمبيوتر Computer Impersonation.

(**) تشمل تزوير البريد الإلكتروني Electronic Mail Forgery (E-Mail Forgery) وتزوير الوثائق والسجلات Document/Record Forgery وتزوير الهوية Identity Forgery.

(***) تشمل تملك وإدارة مشروع مقامرة على الإنترنت Owning and Operating an Inter-net Gambling business وتسهيل إدارة مشاريع القمار على الإنترنت Facilitating the operation of an Internet gambling business وتشجيع مشروع مقامرة عبر الإنترنت Patronizing an Internet Gambling Business واستخدام الإنترنت لترويج الكحول ومواد الإدمان للقصر Using the Internet to provide Liquor to minors و Using the Internet to provide cigarettes to minors و Using the Internet to pro-vide prescription drugs.

## سادساً: جرائم الكمبيوتر ضد الحكومة(*):

**Crimes Against the Government**

كما قامت وزارة العدل الأمريكية بوضع تقسيم في عام ٢٠٠٠ لجرائم المعلوماتية، يشمل تجريم أفعال السطو على البيانات، الاتجار بكلمة السر، انتهاك حقوق الطبع (الافلام والبرامج والتسجيل الصوتى) وعمليات القرصنة، سرقة الأسرار التجارية باستخدام الحاسب الألى، تزوير الماركات التجارية باستخدام الحاسب، تزوير العملة باستخدام الحاسب، نشر الصور الفاضحة واستغلال الأطفال، الاحتيال بواسطة الحاسب(١).

(*) تشمل هذه الطائفة كافة جرائم تعطيل الأعمال الحكومية وتنفيذ القانون Obstructing Enforcement of law or other government iunction والإخفاق فى الإبلاغ عن جرائم الكمبيوتر Failure to report a cyber crime والحصول على معلومات سرية Obtaining confidential government information والإخبار الخاطئ عن جرائم الكمبيوتر False Reports of Cyber Crimes والعبث بالأدلة القضائية Tampering with evidence و Tampering with a Computer Source Document وتهديد السلامة العامة Endangering Public Safety وبث البيانات من مصادر مجهولة Anonymity كما تشمل الإرهاب الإلكترونى Cyber-Terrorism والأنشطة الثأرية الإلكترونية أو أنشطة تطبيق القانون بالذات Cyber-Vigilantism.

(١) ايمن عبد الله فكرى – المرجع السابق – ص ١٠٠.

ومن الأفعال الأخرى المجرمة.

- الإزعاج باستخدام الحاسب.
- فيروس الحاسب.
- استخدام شبكة الحاسب فى ارتكاب الجرائم التقليدية، مثل غسل الأموال والمخدرات.

كما أورد مكتب التحقيقات الفيدرالية تقسيماً للجريمة المعلوماتية فى ٢٠٠٠ قسم فيه هذه الأفعال إلى سبعة أنواع من الجرائم وهى:

- اقتحام بواسطة الحاسب لشبكة الهواتف العامة أو الخاصة.
- اقتحام شبكة الكمبيوتر الرئيسية لأى جهة.
- انتهاك السرية فى بعض المواقع.
- انتهاك سلامة الشبكة المعلوماتية.
- التجسس الصناعى.

=/=

## المطلب الثالث

## الوضع في مصر بالنسبة لتقسيم جرائم المعلوماتية

اجتهد الباحثون فى مصر وأدلو بدلوهم فى معترك البحث عن نموذج قانونى لتجريم الأفعال التى تنتهك النظم المعلوماتية، ومع أن الإجرام المعلوماتى La Crimin alité informatique، أو الاليكترونى électronique كما يفضل البعض نعته، لم يتخذ فى الواقع المصرى بعد - بل والواقع العربى أيضاً - الأبعاد والتفصيلات التى اتخذها فى الولايات المتحدة الأمريكية ودول أوروبا، بل وجانب من دول شرق آسيا - المتنمرة - إلا أن خطورة الوضع تحتم علينا ضرورة العمل الجاد المتواصل للتصدى لهذا النشاط الإجرامى التقنى، حيث أخذت مختلف قطاعات الدولة بتقنية الحاسبات والمعلوماتية، دون دراسة متأنية مستفيضة لسلبيات ومخاطر هذه التقنية، وفى مقدمتها آفة الجريمة المعلوماتية (الاليكترونية) المتولدة عن استخدامها - ولم يغدو المشرع المصرى - فى هذا المعترك التقنى المعلوماتى - إلا أن قام باصدار بعض التشريعات القليلة التى تتصدى للجريمة المعلوماتية فى أجزاء يسيرة(*)، تاركاً باقى الأمر - أن لم يكن برمته - لتطبيق القواعد العامة فى قانون العقوبات، دون تتبع تشريعى متخصص للأفعال المرتكبة وتعد جريمة معلوماتية، فالساحة القانونية تكاد تخلو من نموذج قانونى متكامل يتناول الجرائم المعلوماتية، مما دفع الفقه إلى تسليط

---

- سرقة برامج الحاسب.
- الجرائم الأخرى التى يكون الحاسب العامل الرئيسى فى ارتكابها.

http;// www. elf. org/Legal/Foreign. and local/comp-crime us state. Laws.

(*) مثل القانون رقم ١٥ لسنة ٢٠٠٥ بشأن تنظيم التوقيع الالكترونى ولائحته التنفيذية الصادرة بقرار وزير الاتصالات وتكنولوجيا المعلومات رقم ١٠٩ لسنة ٢٠٠٥، والقرارات المنفذة له. ولم يتضمن القانون - سابق الذكر - سوى مادة واحدة فقط هى المادة ٢٣ التى أوضح فيها المشرع بعضاً من صور الجريمة المعلوماتية، والعقوبة المقررة لها.

الضوء على مشكلة الإجرام فى القطاع المعلوماتى، ولا تثريب عليه فى ذلك إن تناول جانب من جوانب المشكلة، أو تصدى لمعالجة موضوع من موضوعات الجريمة المعلوماتية، مستنيراً فى ذلك بالفقة المقارن الذى أولى هذه المشكلة اهتماماً كبيراً، وأضحى لديه خبرات متنوعة فى الميدان التشريعى لجرائم المعلوماتية.

**أولا: تقسيم الجرائم المعلوماتية تأسيساً على العلاقة بين نظام الحاسب وارتكاب بعض الجرائم:**

حيث ذهب رأى[1] إلى أنه توجد علاقة بين نظام الحاسب الألكترونى La systeme d'ordinateur وارتكاب بعض الجرائم، وذلك نتيجة طبيعية للتطور التكنولوجى الحالى، سواء استخدم الحاسب الألكترونى كمحل للتحايل Objet d'une fraude، أو كان وسيلة للتحايل Moyen d'une fraude.

وقصر هذا الرأى بحثه على جرائم الاعتداء على المال المعلوماتى[*]، موضحاً أن بيان هذه الجرائم ينقسم إلى:

---

(١) د/ هدى حامد قشقوش – جرائم الحاسب الإلكترونى (فى التشريع المقارن) – (مرجع سابق).

(*) إن تحديد الطبيعة القانونية للمال المعلوماتى La nature Juridique de bien informa-tique هى مسألة غاية فى الأهمية فالمال المعلوماتى ينقسم إلى نوعين منفصلين وفقاً لطبيعته فهو:

– إما مال معلوماتى ذو طبيعة معنوية Un bien informatique de nature incorpo-rele، يتمثل ذلك فى البرامج والمعلومات أيا كان موضوعها، سواء تعلقت بالأمن القومى أو الحياة الخاصة أو غيرها.

– وإما أن يكون مال معلوماتى ذو طبيعة مادية Un bien inforamtique de nature cor-porel، ويتمثل فى أدوات وآلات الحاسب الألكترونى الملموسة.

وقد ترتب على الإختلاف فى الطبيعة القانونية للمال المعلوماتى اختلافاً فى النتائج المترتبة على تطبيق بعض نصوص القانون الجنائى التقليدى. (المرجع السابق – ص ٣١).

**أ - الإعتداء علي برامج ومعلومات الحاسب الالكتروني.**

وينقسم هذا الاعتداء استرشاداً بما استحدثه المشرع الفرنسي لأول مرة في القانون رقم ١٩ لسنة ١٩٨٨ إلى:

- جريمة التوصل بطريق التحايل لنظام المعالجة الآلية للبيانات.
- جريمة اتلاف برامج ومعلومات الحاسب الالكتروني.
- جريمة سرقة برامج ومعلومات الحاسب الالكتروني.

**ب- الاعتداء علي أدوات وآلات الحاسب الالكتروني.**

- جريمة اتلاف المال المعلوماتي المادي.
- جريمة الاستخدام الغير مستحق لأدوات وآلات الحاسب الالكتروني.
- جريمة سرقة المال المعلوماتي المادي.

**جـ- جريمة التحايل المعلوماتي.**

**د - جريمة تزوير المستندات الألكترونية.**

**ثانياً: تقسيم الجرائم المعلوماتية من خلال دراسة الجرائم الناشئة عن استخدام الحاسب الآلي:**

فيما ذهب رأي[١] آخر إلى التعرض للجريمة المعلوماتية من خلال دراسة الجرائم الناشئة عن استخدام الحاسب الآلي ، قاصراً ذلك على موضوع جرائم الأموال الناشئة عن إستخدام الحاسب الآلي، حيث تقع الجريمة على الحاسب الآلي ذاته وما يتصل به من ملحقات، أو تقع على أموال الغير بإستخدام الحاسب ذاته.

**أ - الحالات التي تقع فيها الجريمة عن طريق إستخدام الحاسب الآلي كأداة سلبية.**

---

(١) د/ جميل عبد الباقي الصغير – القانون الجنائي والتكنولوجيا الحديثة (الكتاب الأول – الجرائم الناشئة عن استخدام الحاسب الآلي) – مرجع سابق .

– الاستخدام غير المشروع للمعلومات التى يختزنها الجهاز، وقد يتحقق الاستيلاء على هذه المعلومات فى حالتين:

- قبل تشغيل الجهاز – وتتمثل الجرائم التى يمكن أن ترتكب فى هذه المرحلة فى سرقة المعطيات أو إتلاف المعطيات.
- أثناء تشغيل الجهاز – بالاستخدام الناتج عن التشغيل العادى للجهاز، وتتمثل الجرائم التى يمكن أن ترتكب فى التدخل المباشر أو التدخل غير المباشر، أو سرقة ساعات عمل الحاسب الآلى (تشغيل الحاسب الآلى بدون مقابل).

– الاستخدام التعسفى لبطاقات الإئتمان الممغنطة، من خلال أساليب إجرامية جديدة فى مجال المعالجة الآلية للمعلومات: –

- الجرائم التى يمكن أن ترتكب نتيجة اساءة إستخدام العميل للبطاقة.
- استخدام البطاقة غشاً من قبل الغير.

**ب- الجرائم التي تقع بإستخدام الحاسب الآلي كأداة ايجابية.**

– التدخل فى المعطيات.

من خلال تعديل البرنامج، أو خلق برنامج جديد.

– جرائم تقع باستخدام الحاسب الآلى تتضمن اعتداء على الذمة المالية للغير. (السرقة – النصب – خيانة الأمانة).

**ثالثاً: تقسيم الجرائم المعلوماتية تأسيساً علي النظام المعلوماتي:**

فيما ذهب رأى ثالث(1) إلى أن الجريمة المعلوماتية – كما قيل – تقاوم التعريف Resists defintion. ولا أدل على ذلك من أن الكتابات التى تناولتها تحفل – حسب تعبير البعض – «بملايين الكلمات» التى سطرت فى محاولات عديدة لصياغة ودحض تعاريفها(2).

---

(1) د/ هشام محمد فريد رسم – قانون العقوبات ومخاطر تقنية المعلومات – مرجع سابق – ص ٢٩ وما بعدها.

(2) R. E. Anderson, Bank Security, Butterworth (Publishers) INC, 1981, p. 260.

ويختلف موضوع الجريمة المعلوماتية بحسب ما إذا كانت موجهه ضد أحد مكونات النظام المعلوماتى، بحيث يكون هذا الأخير موضوعها، أو مرتكبه من خلال هذا النظام، بحيث يكون هو وسيلة تنفيذها وأدائها.

● ففي الحالة الأولى:

تجتمع الجرائم التقليدية البحتة والجرائم المعلوماتية بمعناها الفنى فتتوافر أولاهما إذا كانت المكونات المادية للنظام - كالأجهزة والمعدات والكابلات - هى محل الاعتداء أو موضوع الجريمة، ولم يكن ثمة أهمية تقنية فى ارتكاب الجريمة، كما هو الحال فى سرقة أو اتلاف الحاسب أو شاشته.

وتتوافر الثانية حينما تكون المكونات غير المادية للنظام(*) - كالبيانات والبرامج فى ذاتها - هى محل الاعتداء، كما هو الحال فى الاعتداء على البيانات المختزنة فى ذاكرة الحاسب أو المنقولة عبر شبكات الاتصال بالسرقة أو التزوير، أو الاعتداء على البرنامج ذاته بادعاء ملكيته أو سرقته أو تقليده أو إتلافه أو محوه أو تعطيله(**).

● وفي الحالة الثانية:

نكون إزاء جرائم تقليدية أداة ارتكابها ووسيلة تنفيذها هى الحاسب أو النظام المعلوماتى عامة[1]. ومن الوجهة النظرية - وكما تشهد بعض الحالات الواقعية -

---

(*) لا يتألف النظام المعلوماتى Systeme informatique من آلات وأدوات مادية فحسب، وإنما هو مجموعة متآزرة تشكل من: عناصر مادية (ملموسة) كأجهزة الحاسبات والدعامات المغنطة والكابلات، وعناصر غير مادية كالبرنامج الأساسى Le logiciel de base الذى يزود به الحاسب قبل طرحه للبيع، والبيانات والبرامج التطبيقية الخاصة بمستخدمه، واطار الاستغلال يتضمن المنظمة وخطة العمل فى مركز معالجة المعطيات.

(**) يطلق البعض على محل الاعتداء فى هذه الصورة تسمية (فن الحاسب الآلى) ابرازاً لماليته المغايرة فى صورتها لصورة المال التقليدى. يراجع: د/ عمر الفاروق الحسينى - تأملات فى بعض صور الحماية الجنائية لبرامج الحاسب الآلى - مجلة المحامى - الكويت - س ١٢ - عدد نوفمبر/ ديمسر ١٩٨٩ - ص ١٣.

(١) د/ هشام رستم - المرجع السابق - ص ١٩.

يمكن استخدام الحاسب لارتكاب طوائف من الجرائم شتى، كجرائم الاعتداء على الذمة المالية (السرقة – النصب – خيانة الأمانة)، وانتهاك حرمة الحياة الخاصة والتزوير والتجسس، وحتى القتل.

والفاعل فى مثل هذه الجرائم هو المتلاعب فى الحاسب ونظامه، أما محلها المادى فيختلف بطبيعة الحال بحسب الشئ الذى ينصب عليه سلوك الفاعل، والذى يشكل محل الحق أو المصلحة المحمية.

وصور الاعتداء الثانية – لا الأولى – هى التى لم يتم – بسبب حداثتها النسبية – معالجتها فى معظم قوانين العقوبات القائمة.

وقد انتهى هذا الرأى إلى أنه ابتغاء للفهم العلمى السليم – والشامل قدر الإمكان – لظاهرة الإجرام المعلوماتى، باعتباره مدخلا وشرطاً مسبقاً لمواجتها قانوناً مواجهة فعالة تكفل الوقوف في وجهها والتقليل من حدة أثارها(١)، وبالنظر لعدم وجود اتفاق عام على تصنيف لميادين الإجرام المعلوماتى، أن يتم الاسترشاد ببعض الدراسات الجادة التى تعرضت له وصفاً وتحليلاً من خلال تصنيفه، بحسب معيار يأخذ فى الاعتبار الأهمية ومعدل التكرار، حيث يتفرع الاجرام المعلوماتى إلى الطوائف التالية:

- الاحتيال المعلوماتى.

أو التلاعب فى أنظمة المعالجة الآلية للبيانات للاستيلاء على المال بالاحتيال.

- قرصنة البرامج، أو نسخها غير المشروع.
- التجسس المعلوماتى فى نطاق قطاع الأعمال.
- التخريب المعلوماتى والإرهاب.
- انتهاك حرمة الحياة الخاصة.

ثم تعرض ذات الرأى للحماية الجنائية للبيانات المعالجة اليكترونيا، مقسماً أيها إلى قسمين:

- الحماية الجنائية للبيانات ذات الصلة بالذمة المالية.

من خلال جرائم (السرقة - النصب - خيانة الأمانة - اتلاف الأموال الثابتة أو المنقولة المملوكة للغير - التزوير فى المحررات - الاستخدام غير المشروع لنظم المعالجة الآلية للبيانات).

- الحماية الجنائية للبيانات ذات الطبيعة الشخصية.

حيث أن تقنية المعلومات فى ثناياها، تحمل مخاطر وتهديدات جدية للأسرار الخاصة بالأفراد وحرمة الحياة الخاصة.

**رابعاً: تقسيم حديث لجرائم المعلوماتية:**

وقد تناول أتجاه حديث[1] دراسة جرائم المعلوماتية من خلال مبدأين أثنين بدأ ظهورهما على يد الفقيه الألمانى Ulrich Sieber، وهما:

- الحق فى المعلومات.
- قانون تقنية المعلومات.

وقد عدل هذا الرأى فى المبدأ الأخير ليكون دراسة هذا الصنف من الجرائم وفقاً لمبدأ الحق فى المعلومات والذى يتم تناوله من خلال حماية سلامة المعلومات من الإتلاف المعلوماتى، وحماية صحة المعلومات من التزوير المعلوماتى، كما تناول الحق على المعلومات من خلال حماية التسلط والاستئثار الوارد على المعلومات من خلال مفهوم ملكية المال المعلوماتى، وحماية الخصوصية المعلوماتية، ليكون تناوله لجرائم نظم المعلومات على الوجه التالى:

**أولاً: الحماية الجنائية للحق في المعلومات.**

ويتم من خلال دراسة:

---

(١) أيمن عبد الله فكرى - المرجع السابق - ص ١٠٩ وما بعدها.

- الحماية الجنائية لسلامة المعلومات (الإتلاف المعلوماتى).
- الحماية الجنائية لصحة المعلومات (التزوير المعلوماتى).

**ثانياً: الحماية الجنائية للحق على المعلومات.**

ويتم من خلال دراسة:

- الحماية الجنائية للملكية المعلوماتية.

من خلال عرض النشاط الإجرامى فى جرائم الأموال والمعلوماتية من:

(السرقة – النصب – خيانة الأمانة).

- الحماية الجنائية للخصوصية المعلوماتية.

**خامساً: تأصيل البيان بشأن ما سبق عرضه من تقسيمات لجرائم المعلوماتية:**

مع سهولة الوصول إلى المعلومات فى النظم المعلوماتية، وتوفر الامكانيات اللامحدودة لتبادلها وإرسالها بصرف النظر عن المسافات والحدود الجغرافية، أدى ذلك إلى نمو هائل فى حجم المعلومات المتاحة، والتى يمكن الحصول عليها. ومع امكانية سوء استخدام خدمات المعلوماتية وتزايد احتمالية ارتكاب أعمال إجرامية فى البيئة المعلوماتية.

وعلى ذلك أضحى على المشرع أن يحافظ على مواكبته لهذه التطورات التكنولوجية، التى تقدم فرصاً واسعة لانحراف استخدام إمكانيات المعلوماتية، وأن يعمل على ردع هذه الأفعال الإجرامية، مع تطبيق سلطات قسرية واضحة ومقررة تحافظ على الاستخدام الأمثل لتكنولوجيا المعلوماتية. ويكون ذلك من خلال تشريع جنائى أمثل، يضم بين مواده كافة الأفعال التى تنال من النظم المعلوماتية. لذلك اجتهد الفقه وأصحاب البحث فى صياغة تقسيمات تلملم الأفعال التى تعد انتهاك لنظم المعلومات، يسترشد بها المشرع فى وضعه لتشريع عقابى لجرائم المعلوماتية. على أنه يتضح تصنيف الفقهاء والباحثون لجرائم المعلوماتية ضمن فئات متعددة، تختلف حسب الأساس والمعيار الذى يستند إليه

تقسيم كل منهم، فذهب البعض لتقسيمها إلى جرائم ترتكب على نظم المعلومات وأخرى ترتكب بواسطتها. والبعض الآخر صنفها ضمن فئات الأسلوب المتبع فى الجريمة، واستند جانب ثالث إلى الباعث (الدافع) لإرتكاب الجريمة، وهناك من يؤسس تقسيمه على تعدد محل الاعتداء وكذا تعدد الحق المعتدى عليه فتوزع جرائم المعلوماتية وفق هذا التقسيم إلى جرائم تقع على الأموال بواسطة النظم المعلوماتية وتلك التى تقع على الحياة الخاصة.

ومن الملاحظ أن هذه التقسيمات أو بعضها، لم تراع بعض أو كل خصائص هذه الجرائم وموضوعها والحق المعتدى عليه لدى وضعها لأساس أو معيار التقسيم. وخلاصة العرض أن جرائم نظم المعلومات فى نطاق الظاهرة الإجرامية المستحدثة هى جرائم تنصب على المعلومات وتطال الحق فى المعلومات، ويستخدم لاقترافها وسائل تقنية تقتضى استخدام نظم المعلومات. وأن الجرائم التى تنصب على الكيانات المادية مما يدخل فى نطاق الجرائم التقليدية ولا يندرج ضمن الظاهرة المستحدثة لجرائم نظم المعلوماتية(١).

**أ - تقسيم الجرائم تبعاً لنوع المعلومات محل الجريمة:**

يتميز هذا التقسيم بأنه الذى توافق مع موجات التشريع فى ميدان قانون تقنية المعلومات، وأنه التقسيم الذى يعكس التطور التاريخى لظاهرة جرائم المعلوماتية، ويتلاحظ أنه التقسيم السائد فى مختلف مؤلفات الفقيه Ulrich Sieber، والمؤلفات المتأثرة به.

ولذا نجد أن جرائم نظم المعلومات استناداً إلى هذا المعيار يمكن تقسيمها إلى الطوائف التالية(٢):

---

(١) أيمن عبد الله فكرى – المرجع السابق – ص ١٠٢.

(٢) المرجع ذاته.

- **الجرائم الماسة بقيمة المعلومات:**

**وتشمل هذه الطائفة فئتين:**

**الأول:** الجرائم الواقعة على ذات المعلومات. كجرائم الإتلاف والتشويه للبيانات والمعلومات وبرامج الحاسب بما في ذلك استخدام وسيلة (الفيروسات) التقنية.

**الثانية:** الجرائم الواقعة على ما تمثله المعطيات آلياً من أموال أو أصول، (كجرائم غش الحاسب) التي تستهدف الحصول على مال، أو جرائم الاتجار بالمعطيات، وجرائم التحرير والتلاعب في المعطيات المخزنة داخل نظم المعلومات واستخدامها (تزوير المستندات المعالجة آلياً واستخدامها).

- الجرائم الماسة بالمعطيات الشخصية أو البيانات المتصلة بالحياة الخاصة.

تشمل جرائم الاعتداء على المعطيات السرية أو المحمية، وجرائم الاعتداء على البيانات الشخصية المتصلة بالحياة الخاصة.

- الجرائم الماسة بحقوق الملكية الفكرية لبرامج الحاسب ونظمه (جرائم قرصنة البرمجيات).

تشمل نسخ وتقليد البرامج وإعادة إنتاجها وصنعها دون ترخيص، والاعتداء على العلامة التجارية وبراءة الاختراع.

- **تقييم هذا التقسيم[1]:**

بدراسة هذا الطوائف، يتلاحظ أن الحدود بينها ليست قاطعة ومانعة، فالتداخل حاصل ومحقق، إذ أن الاعتداء على معطيات الحاسب بالنظر لقيمتها الذاتية أو ما تمثله، هو في ذات الوقت اعتداء على أمن المعطيات، لكن الغرض المباشر المحرك للاعتداء أنصب على قيمتها أو ما تمثله.

---

(١) المرجع السابق – ص ١٠٢.

والاعتداء على حقوق الملكية الفكرية لبرامج الحاسب، هو اعتداء على الحقوق المالية واعتداء على الحقوق الأدبية لكنها تتميز عن الطوائف الأخرى بأن محلها هو البرامج فقط، وجرائمها تستهدف الاستخدام غير المحقق أو التملك غير المشروع لهذه البرامج.

هذا من جهة ومن جهة أخرى، نجد أن الحماية الجنائية للمعلومات فى نطاق القانون المقارن وفى إطار الجهود الدولية لحماية معطيات الحاسب واستخدامه، اعتمدت على نحو خالف التقسيم المتقدم، فظهرت حماية حقوق الملكية الأدبية للبرامج، وحماية البيانات الشخصية المتصلة بالحياة الخاصة، وحماية المعطيات بالنظر لقيمتها أو ما تمثله والذى عرف بحماية (الأموال)، كل فى ميدان وموقع مستقل، وهو فى الحقيقة تمييز بين حماية قيمة المعطيات، وأمنها، وحقوق الملكية الفكرية.(*)

**ب- تقسيم الجرائم تبعاً لدور نظم المعلوماتي في الجريمة:**

دور نظم المعلومات فى الجريمة، ربما يكون محل الاعتداء، بمعنى أن يستهدف الفعل المعطيات المعالجة أو المخزنة أو المتبادلة بواسطة نظم المعلومات والشبكات، وهذا ما يعبر عنه بالمفهوم الضيق (لجرائم المعلوماتية)، وقد يكون الحاسب وسيلة ارتكاب جريمة أخرى فى إطار مفهوم (الجرائم المرتبطة بالحاسب)، وأخيراً قد يكون الحاسب بيئة الجريمة أو وسطها أو مخزناً للمادة الإجرامية.

(*) الملاحظ أن حماية أمن المعطيات (الطائفة الثانية) انحصر فى حماية البيانات الشخصية المتصلة بالحياة الخاصة. أما حماية البيانات والمعلومات السرية والمحمية فقد تم تناوله فى نطاق (الطائفة الأولى) الماسة بقيمة المعلوماتى بالنظر إلى أن الباعث الرئيسى للاعتداء والغرض من معرفة أو إفشاء هذه المعلومات غالباً ما كان الحصول على المال، مما يعد من الاعتداءات التى تندرج تحت نطاق الجرائم الماسة بقيمة المعطيات التى تتطلب توفير الحماية الجنائية للحقوق المتصلة بالذمة المالية التى تستهدفها هذه الجرائم.

وفى هذا النطاق هناك مفهومان يجرى الخلط بينهما يعبران عن هذا الدور[١]:

• **المفهوم الأول: جرائم التخزين:**

يقصد بها تخزين المواد الإجرامية أو المستخدمة فى ارتكاب الجريمة أو الناشئة عنها.

• **المفهوم الثاني: جرائم المحتوي:**

أو ما يعبر عنه بالمحتوى غير المشروع أو غير القانونى.

والأصطلاح الأخير استخدم فى ضوء تطور أشكال الجريمة مع استخدام الإنترنت، وأصبح المحتوى غير القانونى يرمز إلى جرائم المقامرة ونشر المواد الأباحية والغسل الاليكترونى للأموال وغيرها. باعتبار أن مواقع الإنترنت تتصل بشكل رئيسى بهذه الأنشطة.

والحقيقة أن كلا المفهومين يتصلان بدور الكمبيوتر والشبكات كبيئة لارتكاب الجريمة وفى نفس الوقت كوسيلة لارتكابها. وهذا التقسيم شائع - تقسيم الجرائم إلى جرائم هدف ووسيلة - لدى الفقه المصرى والفرنسى[٢]. وتبعا له تنقسم جرائم المعلوماتية إلى جرائم تستهدف نظام المعلوماتية نفسه كالاستيلاء على المعلومات وإتلافها، وجرائم ترتكب بواسطة نظام الحاسب الآلى ذاته مثل جرائم الاحتيال المعلوماتى.

---

(١) المرجع السابق - ص١٠٣.

(٢) انظر على سبيل المثال التقسيمات الواردة لجرائم المعلوماتية لدى: د/ هدى حامد قشقوش - مرجع سابق - ص ٣١ وما بعدها، د/ جميل عبد الباقى الصغير - مرجع سابق، د/ هشام رستم - مرجع سابق. وبالفرنسية أنظر:

- Catala Piere, ebauche Dune Théorie Juridique de, Information, 1983.
- Lucas André, Protection of Information Bases, Kuwait Frist Conference, Ministry of Justice, 15-17 Feb. 1999. Kuwait.

مشار إليه لدى: أيمن عبد الله فكرى - المرجع السابق - هامش ١ - ص١٠٣.

ونلاحظ أن تقسيم الجرائم المعلوماتية كجرائم هدف ووسيلة هو الاتجاه العالمى الحديث فى ضوء تطور النظم التشريعية فى دول أوروبا تحديداً، وأفضل ما يدل على ذلك ما انتهجته الاتفاقية الأوروبية لتقسيم جرائم المعلوماتية(*).

(*) منذ مطلع عام ٢٠٠٠ يتجه العمل على مستوى الفكر الأوروبى إلى وضع إطار عام لتصنيف جرائم نظم المعلومات، وأقل تقدير لذلك وضع قائمة تمثل الحد الأدنى للتعاون الدول فى مجال مكافحة هذه الجرائم، وهذا الجهد وأن كانت دول أوروبا هى التى تقوده فى نطاق فكر أوروبا الموحدة، ولكن بتدخل ومساهمة متزامنة من قبل دول استراليا وكندا والولايات المتحدة الأمريكية.

## المبحث الثاني

## التنظيم القانوني للجريمة المعلوماتية

أهداف كثيرة يحققها بسط الحماية الجنائية للمعلوماتية، من هذه الأهداف فى الجانب الشخصى صيانة أسرار الأفراد فى مواجهة نشرها وتداولها والعبث بمحتواها وتحريف تفصيلاتها، وفى الجانب الموضوعى فإن الحماية الجنائية تنطوى على تأمين استثمارات تكنولوجيا المعلومات فى جوانبها المتعددة سواء المادية أو البشرية أو الإنسانية، مما يشجع على الإبتكارات والتقدم العلمى والتكنولوجى، كما أن هذه الحماية تحقق أهداف التنمية الاقتصادية. وقد تدخل المشرع الفرنسى نحو تنظيم الجوانب القانونية المواجهة للإجرام المعلوماتى بمجموعة القواعد العامة المطبقة على الجرائم التقليدية، عندما تكون الجريمة واقعة على نظم المعلوماتية فى شكلها التقليدى مثل السرقة والاتلاف والنصب، أو من خلال مجموعة القواعد الخاصة بالجرائم المعلوماتية، وكان هذا التنظيم التشريعى الفرنسى سابقاً للعديد من الدول بصفة عامة، وسابقاً على تدخل المشرع المصرى لتناول هذا السلوك الإجرامى ذو التنقيات الحديثة بنصوص عقابية خاصة.

وسوف نتناول موضوع التنظيم القانونى للجريمة المعلوماتية، من خلال المطلبين التاليين:

المطلب الأول: الطبيعة القانونية للمعلوماتية.

المطلب الثانى: النصوص القانونية لحماية المعلوماتية.

## المطلب الأول

## الطبيعة القانونية للمعلوماتية

ترتبط التطورات العلمية الحديثة ارتباطاً وثيقاً بأنظمة المعلوماتية والاتصالات[(١)] ، وتعتمد المعلوماتية فى انتشارها على أنظمة المعلومات. فكلما تقدمت هذه الأنظمة وارتقت كلما اتيح للمجتمع أن ينمو ويتطور ويتقدم، لذلك أصبحت المعلومات وبرامجها وأنظمتها تعد قيمة غير تقليدية، نظراً لاستخداماتها المتعددة فى كافة المجالات الاجتماعية والاقتصادية والثقافية والعلمية[(٢)] . فهذه القيمة المميزة لبرامج التكنولوجية المتطورة من أعمدة الأنظمة الاقتصادية الحديثة، حتى قيل - وبحق - أن المعلوماتية ستعيد تشكيل حياة الإنسان فى هذا القرن[(٣)]. فهو قرن المعلومات[(٤)] .

فالمعلومات بالنسبة لأجهزة الكمبيوتر بمثابة القلب من جسم الإنسان[(٥)] . فهى لها قيمتها السياسية والاقتصادية والثقافية، تلك القيمة جديرة برفعها إلى مصاف الأموال، فيتحدد سعرها بوصفها سلعة قابلة للتداول، خاضعة لظروف العرض والطلب تباع وتشترى، فى سوق يدور فيه الصراع حول مبالغ هائلة[(٦)]، مما أدى إلى ظهور قيمة اقتصادية جديدة وأموال جديدة عرفت بالأموال

---

(1) Azancot (Léon): "La formation du contrat". La gazette du Paris, 24 ' 25 Janvier 1993, p. 29 et 30.

- Lucas (André): "Droit de L'informatique, coll. thémis, PUF. 1987.

(٢) د/ السيد عتيق - جرائم الانترنت - دار النهضة العربية - سنة ٢٠٠٠ - ص ٧٩.

(٣) د/ السيد عطية عبد الواحد - التجارة الالكترونية - بحث مقدم لكلية الحقوق جامعة حلوان - المؤتمر الثانى فى الإعلام والقانون - سنة ١٩٩٩ - ص ١٢.

(٤) د/ سامى الشوا - مرجع سابق - ص ٣٥.

(٥) د/ على القهوجى - الحماية الجنائية لبرامج الحاسب - الدار الجامعية للنشر - الإسكندرية - سنة ١٩٩٤ - ص ٤.

(٦) د/ السيد عتيق - المرجع السابق - ص ٨٠.

لمعلوماتية، وصاحب ظهور هذا المال المعلوماتي جرائم جديدة عرفت بالجرائم لمعلوماتية[1].

**أولاً: الملكية في فضاء المعلومات:**

تمثل الملكية فى فضاء المعلومات تحدياً كبيراً لفقه القانون الجنائى، فنظراً لغياب الطبيعة المادية للمعلوماتية، فقد حدث خلاف فقهى حول امكانية تملك المعلومة، وبالتالى صلاحتها لإمكان خضوعها للحماية الجنائية.

- فذهب رأى إلى أن مستحدثات العصر والتقنيات الحديثة أظهرت ما عرف بالمال المعلوماتي وهذا المال يمكن تملكه[2]، وأنه فى مجال المعلوماتية إذا كان ثمة خلاف حول طبيعة هذا المال هل هو مال مادى أو معنوى[3]، بيد أن الثابت أن هذا المال معرض للاعتداء عليه. فحتى الأشياء المملوكة ملكية معنوية والتى يعترف بها القانون، ترتكز على الاعتراف بأن للمعلومة قيمة، لذلك يجب أن تعامل بوصفها قيمة وتصبح محلاً للحق. فلا يوجد ملكية معنوية بدون الاقرار بالقيمة للمعلوماتية (وهذه القيمة عند الاقتضاء يمكن أن ندفعها إلى مصاف القيمة القابلة لأن تحاز حيازة مشروعة أو غير مشروعة)[4]، فالمعلومة عندما يتم تخليقها أو استحداثها فأنها تخص مالكها، فيكون هو السيد عليها ويمكنه رفض اذاعتها، فالحق فى الحبس خاصية طبيعية للحيازة المشروعة، فعلاقة المعلومة بصاحبها أشبه بعلاقة الابن بأبيه[5].

---

(1) Devéze (J): Le vol de "biens informatiques" J.C.P. 1985. Doctrine -1-3210 - No. 1. Iinemtet droit Penal Pcinis 1998.

(٢) د/ حسام كامل الاهوانى – الحماية القانونية للحياة الخاصة فى مواجهة الحاسب الألى – بحث مقدم لمؤتمر الكويت الأول للقانون والحاسب الآلى – سنة ١٩٩٩ – ص ١٦.

(٣) د/ على القهوجى – المرجع السابق – ص ٥١.

(٤) د/ السيد عتيق – المرجع السابق – ص ٨٢.

مشيراً إلى:

- Devéze (J.), Op. Cit., 1985. p. 16.

(٥) د/ سامى الشوا – مرجع سابق – ص ١٨٧.

- بينما ذهب رأى أخر إلى اتجاه نافياً الحق فى الملكية على المعلومة مؤسساً ذلك على ما أسماه «نظام السماء المفتوحة». متمسكاً بمذهب الحرية فى الاقتصاد الرأسمالى «اتركه يعمل أتركه يمر»، فمالمعلومة لا تقبل التملك والاستثمار، فالانتفاع بها حق للكافة(١). والمعلومات لا يمكن احتكارها وبالتالى لا يمكن تملكها، فالأفكار والمعلومات تسير كما تشاء(٢).

**ثانياً: هل تعتبر المعلومات مالاً يستحق الحماية الجنائية؟**

قبل الخوض فى غمار الحديث عن السؤال السابق، من الأهمية أن بغرض لتعريف المال فى نطاق القانون الجنائى والقانون المدنى، ثم نتعرض لفكرة المال القانونى.

**أ - تعريف المال في القانون الجنائي:**

المال هو عصب الحياة منذ قديم الأزل، ومنذ أن عرفت الملكية الفردية اتجه الإنسان إلى صيانتها من الاعتداء عليها بكل وسيلة، وحيازة الإنسان للمال تزيد فى ذمته المالية وتيسر له سبل الحياة، والاستيلاء على بعضه ينقص من تلك الذمة، مما قد يترتب عليه بعض الاضرار(٣).

فالمال هو كل نافع للإنسان، وما يشبع حاجة للإنسان يسمى مالاً(٤)، ويكون هذا المال مادياً أو معنوياً، تبعاً لما اذا كانت الحاجة التى يشبعها مادية أو معنوية.

---

(1) PATRICK (Nicoleau): La Protection des données sur les autoroutes de L'information, d.S. 1996, 14 e cahier, chron, p. 112.

(٢) د/ هشام رستم - مرجع سابق - ص ٢٥٦.

(٣) د/ حسن صادق المرصفاوى - جرائم الأموال - مطبعة نهضة مصر - سنة ١٩٥٦ - ص ٣.

(٤) د/ رمسيس بهنام - نظرية التجريم فى القانون الجنائى - منشأة المعارف - الإسكندرية - سنة ١٩٩٦ - ص ١٠٠.

وجاء فى نص المادة ٣١١ عقوبات مصرى أنه لا تقع جريمة السرقة إلا على مال مادى منقول. مفهوماً على أنه كل شئ ذى كيان مادى ملموس يصلح فى نظر القانون لأن يكون محلاً للتملك، وبالتالى لا يصلح محلاً لسرقة الأموال المعنوية،، كالأفكار والآراء والإبتكارات، لأنها ليست منقول مادى يمكن إنتزاعه. ولكن المحررات المثبتة لهذه الأموال المعنوية – نظراً لكونها أشياء مادية – هى التى يمكن أن تكون موضوعاً للسرقة[١].

وفى ذات السياق اعتبرت القوة الكهربائية مال منقول[٢]، وهذا ما ذهبت إليه محكمة النقض المصرية[٣]، حيث قضت بأن التيار الكهربائى مما تتناوله كلمة منقول، إذ المنقول هو كل شئ ذى قيمة مالية يمكن حيازته ونقله، وهذه

---

(١) د/ جميل عبد الباقى الصغير – القانون الجنائى والتكنولوجيا الحديثة – دار النهضة العربية – سنة ١٩٩٢ – ص ٥٢. وأيضاً يراجع:

- Crim., 24 Juin 1965, J.C.P. 1966, 2, 114700, Note BECOURT. Paris.

(٢) قضت المحاكم الفرنسية بأن بعض القوى مثل الكهرباء هى أشياء، وبالتالى يمكن أن تكون محلاً للسرقة.

- Crim., 3 Août 1912, D 1913, I,P. 349, S. 1913, I. P. 337, Note roux, R.S.C., 1950, P. 208, obs BOUZAT, 12 Juin 1929, G.P. 11929, 2, p. 251.

وهذا هو رأى البعض من الفقه الفرنسى الذى يرى أن الكهرباء لها كيان مادى يمكن حيازته ومباشرة كافة السلطات عليه. ومن ثم التصرف فيه.

- GARRAUD (René): "Traité théorique et Pratique de droit Pénal" tome 4, 3 éme édition, 1913 à 1952, n °2375. p. 112.

مشار إليه لدى د/ جميل عبد الباقى الصغير – المرجع السابق – هامش ٣ – ص ص ٥٢، ٥٣.

(٣) نقض ١٦ أبريل ١٩٣١ – مجموعة القواعد القانونية – جـ٢ – رقم ٤٤ – ص ٢٩٨.
نقض ٥ أبريل ١٩٣٧ – مجموعة القواعد القانونية – جـ٤ – رقم ٦٣.
نقض ١٧ ديسمبر ١٩٥٢ – مجموعة أحكام محكمة النقض – س ٣ – رقم ٨١ – ص ٢٠٥.
نقض أول أكتوبر ١٩٦١ – مجموعة أحكام محكمة النقض – س ١٧ – رقم ١٥٢ – ص ٧٨٨.

الخصائص متوفرة فى الكهرباء، ويطبق هذا المبدأ أيضاً على كل قوة أو طاقة يمكن أن تخضع لسيطرة الإنسان، ويكون بوسعه أن يوجهها على النحو الذى يحقق منفعة، ومن هذه القوى (القوى النووية)(١).

ب- تعريف المال في القانون المدني:

جاء بمذكرة المشروع التمهيدى.. وضع المشروع بهذه المادة أساس التفرقة بين الأشياء والأموال، فبين أن الشئ غير المال وأنه لا يعدو أن يكون محلاً للحقوق المالية بشرط الا يكون خارجاً عن التعامل بطبيعته أو بحكم القانون، والأشياء التى تخرج عن التعامل بطبيعتها هى التى ينتفع بها كل الناس بغير أن يحول انتفاع بعضهم دون البعض الآخر، والأشياء التى تحرج عن التعامل بحكم القانون هى التى ينص القانون على عدم جواز التعامل فيها بوجه عام(٢).

فالمال فى القانون المدنى هو كل شئ يصلح فى ذاته لأن يكون محلاً لحق مالى يدخل فى تقدير ذمة شخص طبيعى أو اعتبارى(٣). بمعنى أنه كل شئ قابل للتقوم، ويكون الشئ كذلك اذا صلح محلاً لحق من الحقوق المالية(٤)، طبقاً لنص المادة ١/١٨٨ يستلزم أن يكون داخلاً فى دائرة التعامل وليس خارجاً عنها «هو كل شئ غير خارج عن دائرة التعامل بطبيعته أو بحكم القانون» فاشتراط كون الشئ مالا فى القانون المدنى يتطلب أن يكون (متقوماً)(٥).

بمعنى أنه يشترط أن يكون ذا قيمة، وذلك ان اشتراط صلاحية الشئ لأن يكون محلاً لحق مالى يعترف به القانون، يتضمن اشتراط تمثيله قيمة يمكن

---

(١) د/ محمود نجيب حسنى - شرح قانون العقوبات (القسم الخاص) - ط سنة ١٩٨٧ - رقم ١١٠٠ - ص ٨١٦.

(٢) د/ السيد عتيق - مرجع سابق - ص ٨٥.

(٣) انظر فى تعريف المال - المادة ٨١ من القانون المدنى.

(٤) نقض ٩ أكتوبر ١٩٨٤ - أحكام محكمة النقض - س ٣٥ - ق ١٤٢ - ص ٦٥١.

(٥) د/ جلال ثروت - نظم القسم الخاص - (جرائم الاعتداء على المال المنقول) - دار المطبوعات الجامعية - سنة ١٩٩٥ - ص ٣١.

التعبير عنها بمبلغ من النقود، كذلك المال فى القانون المدنى يصح أن يكون مادياً أو معنوياً لأن الحق المالى قد يرد على شئ مادى أو معنوى، فالمال فى عرف القانون هو كل شئ متقوم نافع للانسان يصح أن يستأثر به وحده دون غيره، وكما يكون المال شيئاً مادياً كالاعيان التى تتحقق بالحواس، ويكون شيئاً معنوياً كالحقوق التى لا تدراك الا بالتصور[1].

- اختلاف فكرة المال في القانون الجنائي عن القانون المدني:

لا يشترط فى القانون الجنائى ان يكون المال خارج عن التعامل بحكم القانون، ولا يشترط أن يكون ذا قيمة يمكن التعبير عنها بالنقود.

بينما القانون المدنى يعتبر المال متقوماً فقط اذا كان يمكن تقديره بمبلغ من النقود، وهذه هى النظرية الاقتصادية. وليس الأمر كذلك فى القانون الجنائى، فالنظر إلى قيمة المال هو نظرة قانونية وليست نظرة اقتصادية[2]. فالمال فى نظر ا لقانون الجنائى ينظر إليه من نطاق فكرة القيمة التى يمثلها المال فى القانون الجنائى، بيد أنه اذا انتفت عن الشئ كل قيمة فلم يعد متقوما زالت عنه صفة المال[3].

كما يشترط فى المال أن يكون ذو طبيعة مادية محسوسة، ويرجع السبب فى ذلك إلى أن القانون الجنائى لا يحمى حق الملكية بوصفه حقاً عينياً مجرداً يتمثل فى سلطات ومكنات قانونية للمالك على ما يملك، وإنما بوصفه تسلطاً مادياً من المالك على ما يملك وهذا يفترض مكان (حيازة) المال المملوك

---

(١) نقض مدنى ٣١ يناير ١٩٤٦ . مشار إليه لدى: أ/ محمد كمال عبد العزيز – التقنين المدنى فى ضوء الفقة والقضاء – ط ٢ – بدون سنة نشر – ص ٢٢١.
(٢) د/ جلال ثروت – المرجع السابق – ص ٣٤.
(٣) د/ محمود نجيب حسنى – المرجع السابق – ص ٨١٢.

والحيازة لا ترد إلا على شئ مادى، فالشئ المادى هو الشئ الذى يتقبل السلطات المادية التى تنطوى عليها الملكية والحيازة(١).

جـ- المال القانوني(*):

ظهرت فكرة المال القانونى على يد الفقيه الالمانى (فون ليست) Von Liszt الذى ذهب إلى أن قانون العقوبات يستهدف حماية أموال معينة يرى الشارع جدارتها بتلك الحماية(٢)، ثم تناولها الفقيه الايطالى (روكو) Rocco الذى عرفها بأنها كل ما من شأنه أشباع حاجة معينة(٣)، فالشئ الصالح لاشباع حاجة ما يعتبر لهذا السبب مالا، فالمنفعه اذا قوام المال. فالأموال تنقلب إلى مصالح فى علاقتها بالإنسان، ويقدر تمكنها من اشباع حاجاته. وفى عبارة أخرى فإن المصلحة هى الرغبة فى الأشياء أو الأموال لأشباع الحاجات(٤).

---

(١) د/ جلال ثروت – المرجع السابق – ص ٣٨.

(*) كان ظهور فكرة المال القانونى لأول مرة منذ أخريات القرن التاسع عشر على يد (Von-Liszt). راجع فى الموضوع:

د/ رمسيس بهنام – فكرة القصد وفكرة الغرض والغاية فى النظرية العامة للجريمة والعقاب – مجلة الحقوق – السنة السادسة – العددان ١، ٢ – ص ٤٥ وما بعدها، د/ عبد الفتاح مصطفى – القاعدة الجنائية – منشأة المعارف – الإسكندرية – سنة ١٩٦٧ – رقم ١١ – ص ٣٥ وما بعدها، د/ حسنين عبيد – النظرية العامة للظروف المخففة – كلية الحقوق – جامعة القاهرة – سنة ١٩٧٠ – رقم ٥٩ – ص ١٠٩.

- Malinverni (Alessandro): Circostanze del reato. Enciclopidia del diritto, 1969, vol. VI n. 4 p. 70 e 71.
- Marini (Guiliano): Circotanze del reato Parte Generale. Milano. 1965, m.3 p. 9.

(٢) د/ ثروت أنيس الاسيوطى – فلسفة التاريخ العقابى – مجلة مصر المعاصرة – القاهرة – العدد ٣٣ – سنة ١٩٦٩ – ص ٢٥٧.

(٣) د/ رمسيس بهنام – المقال السابق – ص ٤٦.

(٤) د/ حسنين صالح عبيد – فكرة المصلحة فى قانون العقوبات – المجلة الجنائية القومية – العدد الثانى – يوليو ١٩٧٤ – المجلد ١٧ – ص ٢٣٧.

فالمصلحة هى العلاقة بين المال والشخص، بمعنى أنها تقييم لتلك العلاقة بين حاجات الفرد وبين الوسائل التى تستخدم لاشباعها(*) . ونخلص من ذلك أن المصلحة هى محل الحماية القانونية وليس المال(**)، وبالتالى فالحماية القانونية تنصرف إلى المصلحة دون المال لتجعل منها مصلحة قانونية، أى مصلحة محمية بنصوص قانون العقوبات(١) .

---

(*) حياة الإنسان أنما تقوم على أشباع حاجات معينة تمليها عليه غرائزه، لأن كل غريزة يتولد عنها بحكم الفطرة شعور بحاجة أو أكثر، بحيث يغدو إشباعها من مقتضيات المعيشة وتختلف الأموال باختلاف الحاجات الإنسانية سواء كانت مادية أو معنوية، وهى قد تتعلق بالعالم المادى الخارجى كالمطر، أو بالحالة الحسية للفرد كالحياة، أو بالعلاقة بين شخصين كالزوجية، أو بالحالة الواقعية كسكون الليل، أو الحالة المتصلة بالشئ كاغلاق حرز أو تسوير مكان، وقد يكون المال ذا قيمة معنوية كالعقيدة، كما قد يتصل بصفة من الصفات كالموظف العام أو الزوج. (د/رمسيس بهنام – المقال السابق – ص ٤٧) .

وإذا كانت الغرائز هى التى تولد الحاجة، فإن الشعور بهذه الحاجة هو الذى يحرك الرغبة والارادة صوب النزوع إلى اشباعها، فغريزة التملك هى التى تولد الحاجة إلى اقتناء العديد من الأموال (عقارية أو منقولة)، والشعور بهذه الحاجة هو الذى يدفع الشخص إلى البحث عن كافة أوجه أكتساب الملكية.

وقد عرف روكو Rocco الحاجة بأنها: «مقتضيات وجودنا، أو إحدى ضرورات الحياة الإنسانية سواء كانت عضوية أو ذهنية أو أدبية» . نقلاً عن Pannain فى مرجعه:

- Pannain (Remo): Manuale di diritto Penale 3a edizione. Torino, 1962. n. 12, p. 26.

مشار إليه لدى: د/ حسنين عبيد – المرجع السابق – ص ٢٣٨ .

(**) واستناداً إلى ما تقدم نستطيع تعريف المصلحة بأنها: «العلاقة بين شخص ومال»، أو هى «الحكم التقييمى الذى يسبغه صاحب الحاجة على الوسيلة التى تكفل اشباعها بصورة مشروعة» .

- Carnelutti. (Francesco): teoria generale del reato, roma 1933, p. 249.

- Pannain: Op. cit., p. 20 note (4).

وأيضاً: د/ رمسيس بهنام – المقال السابق – ص ٤٩، د/ ثروت أنيس – المقال السابق – نفس الموضع. مشار إليه لدى: د/ حسنين عبيد – المرجع السابق – ص ٢٣٩ .

(١) المرجع السابق – ص ٢٤٠ . وتجدر الإشارة إلى أسبقية الفقه الإسلامى عن الفقه الغربى فى جعله المصلحة أساساً للشرع الإسلامى – يقول الشاطبى فى الموافقات: «إن وضع الشرائع إنما
=/=

وعلى الرغم من وضوح التفرقة بين المال والمصلحة، فإن جانباً من الفقه يستعملهما كمترادفين(١)، فيما ذهب رأى أخر(٢) إلى الفصل بينهما أستناداً إلى تحليل كلتا الفكرتين فضلاً عن أن فكرة المال ذات طبيعة موضوعية Oggettiva تعتمد على أهلية Capacità أو جدارة Idoncità المال لإشباع حاجة معينة. بينما المصلحة ذات طبيعة شخصية Soggettiva قوامها تقدير صاحب الحاجة لمدى صلاحية المال لإشباعها.

وبعد أن تعرضت الدراسة لتحديد صفة المال فى التشريع الجنائى، نعود للرد على تساؤل هل المعلومات تبعاً لذلك تعتبر أموالاً تستحق الحماية القانونية؟

أختلف الفقه في هذه المسألة إلى اتجاهيين ذهب الأول إلى أن المعلومات لا تعتبر مالاً، بينما يرى الثانى أن المعلومات تعتبر مالا جديرة بالحماية والسرية، وإن كان فى تناول هذه المسألة من خلال تقسيم المعلوماتية إلى المكونات المادية لنظم المعلومات والمكونات غير المادية أكثر وضوحاً ورؤيا.

**أ - بالنسبة للمكونات المادية لنظم المعلومات:**

لا تثير المكونات المادية لنظم المعلومات أدنى مشكلة من ناحية تكيفها القانونى، والعقاب كجزاء للاعتداء عليها، وذلك فيما اذا كان محل الاستيلاء أجزاء ومكونات مادية، مثل الأسلاك والأجهزة والمعدات التى يتكون منها النظام المعلوماتى، سواء آكانت وسائل ادخال أم معالجة أم إخراج لنتائج النظام المعلوماتى(٣)، بالنظر إلى أن برامج الحاسب الآلى فى بداتيها تعد شيئاً معنوياً،

---

= هو لصالح العباد فى العاجل والآجل معاً. يراجع أبو اسحق إبراهيم بن موسى الشاطبى - الموافقات فى أصول الشريعة.

(1) Grispigni (Filippo): diritto Penale Italiano - II - Milano. 1952. p. 71.
- Dologu (Tullio): Les Causes de Justification. Lecaire. 1952, n. 3. p. 9.

(٢) د/ حسنين عبيد - المرجع السابق - ص ٢٣٩.

(3) Sieber urlich: op. cit., p. 53. Bertrand (G.F.): La Criminalité informatique, Las délits relatif au matériel, expertises, Juin, 1984, p. 150.

وبالتالى لا يصدق عليها وصف المال المادى طبقاً للمفهوم التقليدى. أما اذا سجل البرنامج أو تم إيجاده على دعامة مادية، فإنها منفصلة عن البرنامج تصلح محلاً لجرائم الأموال، وذلك لتوافر شروط المال فيها من حيث المادية والقيمة.

وبالرغم من ضآلة قيمة الدعامة بالنسبة للبرنامج المخزن عليها، وبالرغم من أن الاعتداء على الدعامة ليس غاية فى ذاته، وإنما الباعث هو البرنامج نفسه لا دعامته، إلا أن القانون الجنائى لا يعتد بالبواعث على ارتكاب الجريمة، ويعتبر الاعتداء فى تلك الحالة منصباً على الشئ المادى(*)، ويكيف الفعل بحسب النشاط الإجرامى الذى اقترفه الجانى(١).

فالدعامة المادية التى تحتوى على المعلومات، والتى تم طباعتها كنسخة أصلية، وإعيد نسخها بطريق غير مشروع، يتوافر فيها فعل ونشاط الاختلاس طالما وقع الاعتداء على الدعامة المادية.

ب- المكونات غير المادية للمعلومات:

ثار جدلٌ طويلٌ حول الحماية القانونية للمعلومات فى حد ذاتها، منظوراً إليها استقلالاً عن الوسيط المادى الذى يمكن أن تندمج فيه. فعل الرغم من الأهمية الاقتصادية للمعلومات، فإنها تظل مجرد أفكار غير قابلة للسرقة، أو أن تكون هذه المعلومات محلاً لبعض الجرائم مثل النصب أو الاختلاس أو التقليد. وقد لا يتوافر فى المعلومات – موضوع الاعتداء – مقومات الملكية الفكرية، حتى تشملها النصوص الجنائية بالحماية القانونية لهذا النوع من الملكية.

---

(*) المعلومات غير مادية، ولكنها عندما تكون مسجلة على دعامات مادية من شرائط ممغنطة، أو مخزنة على ديسكات، فهى تأخذ صورة المال المادى، وتصلح محل للسرقة.

(١) د/ على عبد القادر القهوجى – الحماية الجنائية لبرامج الحاسب الآلى – مرجع سابق – ص٤٧.

وقد أدى الخلاف الفقهى فى هذا الشأن الى أنقسام الرأى حول قابلية المعلومات فى ذاتها لأن تكون محلاً لجرائم الاعتداء على الأموال.

**الاتجاه الأولي: المعلومات لا تعتبر مالاً:**

ذهب هذا الاتجاه إلى أن المعلومات ليس لها طبيعة مادية(1). فالأشياء المحسوسة هى التى تعتبر من قبيل الأشياء المادية(2). ولغياب هذا الكيان المادى للمعلومات لا يجعلها محلا لحق مالى من نوع الحقوق المتعارف عليها فى الفقه والتى ترد على كيانات مادية(3). لذلك يلزم بالضرورة استبعادها من طائفة الأموال(4)، فعدم مادية المعلومة هو الذى أدى بهذا الرأى إلى استبعادها من طائفة الأموال، فوصف القيمة لا يضفى إلا على الأشياء المادية والأشياء التى توصف بالقيم هى تلك القابله للاستحواز، فالمعلومات طبيعتها معنوية فانها غير قابلة للاستئثار وبالتالى لا تندرج فى مجموعة القيم.

فبرامج المعلومات عمل ذهنى(5). والبرامج بهذا الفهوم تدخل فى نطاق مجال الأحكام الخاصة بحماية الملكية الفكرية. والمعلومة بعيداً عن دعامتها لا

---

(1) Cass. Crim. 29 avril 1989, J.C.P., 1987, 11, 20788, obs Croze (H.).

(2) DURHAM (Cole): "The Emerging Struc Tures of Criminal information Law: Tracing The contours of a New Poradign" R.I.D.P. 1993, p. 111.

(٣) د/ عبد العظيم مرسى وزير – شرح قانون العقوبات (القسم الخاص – جرائم الاعتداء على الأموال) – مرجع سابق – ص ٤١.

(4) Goutal (Jean - Louis), "Informatique et Driot Prive" in Bensoussan (Alain), Linant de Bellefonds (Xavier), Maisl (Herbert) (eds), emergence du droit de L'informatique, 1983, p. 92,

د/ على القهوجى – مرجع سابق – ص ٥٠، د/ عبد العظيم مرسى وزير – المرجع السابق – ص٤٢.

(5) VIVANT (M.) et Autres: "Droit de L'irformatique" Paris, 1993, p. 56.

تقل التملك والاستئثار، فالانتفاع بها مباح للكافة، وبالتالى لا يمكن أن تكون محلاً للملكية الفكرية[1].

إلا أن استبعاد المعلومات من نطاق القيم المالية، لم يمنع الفقه والقضاء الفرنسى من محاولة إيجاد حماية قانونية لها فى حالة الاستيلاء غير المشروع عليها، ولقد اتخذت هذه المحاولة عدة أشكال تنوعت بين الاستعانة بدعوى المنافسة غير المشروعة، والتطبيق الموسع لنظرية التصرفات الطفيلية، وتأسيس الخطأ على نظرية الإثراء بلا سبب، وأخيراً تأسيسه على فكرة المسئولية التقصيرية.

**الاتجاه الثاني: المعلومات مالاً:**

اتجه رأى أخر إلى امتداد وصف المال المادى إلى المعلومات فى حد ذاتها، على سند من القول بأن المعلومات من طبيعة مادية. وسنده فى ذلك أنه لا يجوز الخلط بين طبيعة حق صاحب الشئ وطبيعة الشئ ذاته، فليس بالضرورة اذا كانت طبيعة حق صاحب الشئ على الشئ معنوية أو ذهنية ان تكون طبيعة هذا الشئ ذاته معنوية فهذا رابط حيث لا رابطة اذ أنه لا لزوم له، وان الفيصل فى ذلك هو تحديد كلمة المادة فى العلوم الطبيعية، فالمادة فى العلوم الطبيعية هى كل ما يشغل حيزاً مادياً فى فراغ معين وان هذا الحيز يمكن قياسه أو التحكم فيه، وبالتالى فإن البرامج فى الكمبيوتر تشغل حيزاً مادياً يمكن قياسه بمقياس معين هو البايت والكيلوبات والميجابايت. وقد يؤيدى هذا القول ان هذه البيانات تأخذ شكل نبضات الكترونية تمثل الرقم صفر واحد (٠ – ١)، وهى فى هذا تشبه التيار الكهربائى الذى اعتبره الفقه والقضاء فى فرنسا ومصر من قبيل الأشياء المادية[2].

---

(١) د/ السيد عتيق – مرجع سابق – ص ٨٩.

(٢) د/ هلالى عبد اللاه أحمد – تفتيش نظم الحاسب – مرجع سابق – ص ٨٥ وما بعدها.

فالمعلومات التى لا تكون متصله بالدوا حى الفنية والأدبية، ولا تشملها حماية الملكية الفكرية، ليس من المقبول أن تظل عارية من أية حماية، اذا ما جرى الاستيلاء عليها، أو استخدامها بطريقة غير مشروعة، فمثل هذا الفعل يعد خطأ يحرك مسئولية فاعله(*).

وقد تبنى جانب من الفقه الفرنسى اتجاه اعتبار المعلومات قيمة تضاف إلى غيرها من القيم الأخرى، وعلى رأسهم الأستاذ "Pierre Catala"، والأستاذ "Michel Vivant"[1].

حيث ذهب "Catala" إلى أن المعلومات فى ذاتها قيمة مالية أشبه بالسلعة، فهى نتاج لعمل بشرى تنتمى ويحسب الأصل، إلى من يحوز العناصر المكونة لها بطريقة مشروعة، ثم يضعها فى شكل ما حتى يمكن أن تكون صالحة للأطلاع عليها وتبليغها بشكل مفهوم[2].

ويرى "Vivant" أن المعلومات قيمة قابلة للتملك لما لها من قيمة اقتصادية لا يمكن النزاع بشأنها، فهى يمكن أن تكون محلاً لعقد بيع. وفى نطاق الملكية الفكرية التى يحميها القانون، فإن المعلومة تكون ذات قيمة من الناحية القانونية[3].

---

(*) أقام جانب من الفقه الفرنسى هذه المسئولية على قواعد المسئولية المدنية وفقاً لنص م ١٣٢ من القانون المدنى الفرنسى، وهو ما أخذت به محكمة النقض الفرنسية، فإنه بالاعتراف بالخطأ تكون المحكمة قد اعترفت بوجود هذا الحق (الحق على المعلومات)، وهذا مؤداه ان يكون للمعلومات طبيعة خاصة تسمح بأن يكون الحق الوراد عليها من نوع الملكية العملية.

(د/ عبد العظيم وزير – المرجع السابق – ص ص ٤٢ ، ٤٣).

(١) د/ نائلة قورة – مرجع سابق – ص ١١٤.

(2) Catala (Pierre): Ebauche d'une Théorie Juridique de L'Information, d., 1984, chr. p. 97.

(3) Vivant (Michel): Apropos des Biens Informationels, J.C.P. 1984, 1. 3132.

فالمعلومات طائفة جديدة من الأموال مما يمكن ان ترد عليها الحقوق المالية، مما حدى ببعض التشريعات الأجنبية إلى اعتبار المعلومات بمثابة جزء من الذمة المالية للشخص، فلا يميزون بين الاعتداء الذى يقع على الذمة المالية وبين الاعتداء الذى يقع على المعلومات أو البيانات. فقد اصدرت بعض الولايات المتحدة الأمريكية قوانين تعرف المال بأنه كل شئ له قيمة مالية، وهذا التعريف يشمل الأموال المادية والمعنوية، لذلك يجب معاملتها على أنها مال، فالشخص الذى يستولى عليها يستطيع استغلالها ويترتب على ذلك حرمان صاحبها الشرعى من عائدها المادى، ثم ان مال له قيمة اقتصادية ضخمة مثل المتعلقة بالأسرار التجارية والصناعية يجب حمايته جنائياً(١).

ويرى الفقه الحديث ان المعيار فى اعتبار الشئ مالا ليس على أساس ماله من كيان مادى وإنما على أساس قيمته الاقتصادية(٢)، وان القانون الذى يرفض اسباغ صفة المال على شئ له قيمة اقتصادية هو بلا جدال قانون منفصل عن الواقع، فتحديد مفهوم الشئ أو المال نابع من الذهن وليس المال، ومما يؤكد صحة هذا القول ان المشرع يعترف لصاحب هذه المعلومات بما يطلق عليه الحق فى الملكية الذهنية والأدبية(٣). فالمعلومة ترتبط بصاحبها عن طريق علاقة قانونية تتمثل فى علاقة المالك بالشئ الذى يملكه. وأنه اذا كان من المهم الأخذ فى الاعتبار الشكل الذى تتجسد فيه المعلومات، فإن القيمة الحقيقية لها تكمن فى ذات المعلومة وليس مجرد الأوراق المكتوبة أو المسجلة عليها(٤).

---

(١) د/ جميل عبد الباقى الصغير – القانون الجنائى والتكنولوجيا الحديثة – دار النهضة العربية – ص ٥٧.

(2) VIVANT (M.): op. cit., p. 2142.

(٣) د/ على القهوجى – مرجع سابق – ص ٥٠.

(٤) د/ جلال وفاء محمدين – فكرة المعرفة الفنية والأساس القانونى لحمايتها – دار الجامعة الجديدة – سنة ١٩٩٥ – ص ٩٥.

كل ذلك أدى إلى رفع المعلومة منظوراً إليها لذاتها إلى مصاف القيم، والواجب حمايتها جنائياً[1].

فالقيمة القانونية تعنى القيمة المرتبطة بالشئ، بحيث تجعل صاحبه حريصاً على اقتنائه، وعلاوة على ملكيته له لاعتبارات مالية أو غير مالية (عاطفية، قومية، روحية)، هنا يعترف القانون بقيمتها ويسبغ عليها الحماية القانونية، بمعنى أن القانون الجنائى ينظر إلى «القيمة» نظرة قانونية وليست نظرة اقتصادية، وهى محل الحماية الجنائية[2].

فإذا كان المشرع يتخير مجموعة من المصالح التى يراها جديرة بالاهتمام والرعاية حفاظاً على مصالح الأفراد وبقاء المجتمع ويرفعها إلى مصاف القيم، لذلك يتدخل جنائياً بحمايتها بفرض عقوبة على من يعتدى عليها[3]. فنظراً لنطبيعة الحمائية لقانون العقوبات الخاص اذ هدفه حمايه مصالح قانونية عجز أو قصر فرع آخر من فروع القانون عن حمايتها[4]، لذلك يصبح من الضرورى تدخل المشرع الجنائى لحماية هذه النوعية الجديدة من الأموال وهى الأموال المعلوماتية، وفرض عقوبة فى حالة الاعتداء عليها، مع ضرورة تحديد هذه الجرائم على سبيل ا لحصر اعمالاً لمبدأ الشرعية الجنائية.

---

(١) د/ السيد عتيق – مرجع سابق – ص ٩١.

حيث ذهب إلى الحاجة لتدخل المشرع الجنائى لحماية المال المعلوماتى، موضحاً أن الرأى بأن القانون الجنائى لم يوضع إلا لحماية أموال معينة رأى غير سليم، فالصحيح ان الحماية القانونية تنصرف إلى المصلحة «القيمة» دون المال لتجعل منه مصلحة قانونية. فمحل الحماية القانونية هو المصلحة وليس المال.

(٢) د/ جلال ثروت – مرجع سابق – ص ٣٦.

(3) Tulio Deiogu, La loi Pénal et son application, Cours.
.De doctorat, 1956, N°, 16.

مشار إليه لدى: (د/ السيد عتيق – المرجع السابق – ص ٩٣٥.

(٤) د/ سليمان عبد المنعم – قانون العقوبات (القسم الخاص) – دار الجامعة الجديدة – سنة ١٩٩٣ – ص ٢٥.

## المطلب الثاني

## النصوص القانونية لحماية المعلوماتية

### الفرع الأول

### النصوص القانونية المطبقة علي جرائم المعلوماتية

### ( في فرنسا )

عندما اتضح جلياً للمشرع الفرنسى أن المعلوماتية أصبحت من وسائل ارتكاب الجرائم ضد الأشخاص والأموال وأن الجهات الإدارية والسلطات العامة فى الدولة ذاتها من الممكن أن تستخدم المعلوماتية فى الافتئاء على حريات وحقوق الأفراد، أصبح لزاماً عليه أن يتدخل بالأسلوب التشريعى لحماية مصالح الناس وحرياتهم. ويقصد بالتدخل التشريعى هنا التدخل عن طريق سن قوانين عقابية يقرها المشرع بالأسلوب المعمول به فى فرنسا(١).

والواقع أنه فيما يخص الجرائم المعلوماتية فإن قانون العقوبات الفرنسى يحتوى على نوعين من القواعد: النوع الأول يشمل مجموعة القواعد العادية والتى يمكن أن تنطبق فى حالة ما اذا كانت الجريمة واقعة على المكونات العادية لنظم المعلوماتية مثل السرقة والاتلاف وخيانة الأمانة... الخ. وهذه الجرائم لا تختلف عن الجرائم العادية فهى تأخذ حكمها(*). أما النوع الثانى فيشمل مجموعة القواعد الخاصة بجرائم المعلوماتية، والتى تمت اضافتها عندما استفحلت ظاهرة الإجرام المعلوماتى. والحقيقة أنه قد تمت اضافة هذه القواعد الى قانون العقوبات على مراحل ثلاثة اعتباراً من عام ١٩٧٨(٢): -

---

(1) Voir aussi en ce sens:

- Emmanuel Dreyer: "Droit de l'information", Responsabilité Pénale des médias, Éditions Litexc, Libraire de La cour de cassation 27, Place Dauphine - 95001 Paris, 2002.

(*) وسوف نرى أنه فى مصر فإن ا لنصوص العامة فى قانون العقوبات والمتعلقة بهذه الجرائم، تطبق هى نفسها بطريق القياس على جرائم المعلوماتية، نظراً لعدم وجود قواعد خاصة بهذا النوع من الجرائم، التى ما أضحت تعتبر جديدة على المجتمع المصرى.

(٢) د/ أحمد حسام طه تمام - الجرائم الناشئة عن استخدام الحاسب الآلى (دراسة مقارنة) - دار النهضة العربية - سنة ٢٠٠٠ - ص ٨١ وما بعدها.

في المرحلة الأولى، صدر قانون ٦ يناير ١٩٧٨ المتعلق بالمعلوماتية والحريات Loi Sur L'informatique, Les fichiers et libertés والواقع أن هذا القانون كان قاصراً على حماية ما يسمى بالمعلومات الأسمية Informations Nominatives ولهذا السبب فإن الحماية التى يقدمها قد اقتصرت على حماية الشخصية Identité والحرية Liberté وسرية الحياة الخاصة للأفراد Le secret de la vie privée des péresonnes[1] وقد استحدث قانون ٦ يناير ١٩٧٨ جرائم جديدة لردع مخالفة أحكامه، فالمسئول عن التعسف فى معالجة المعلومات الاسمية يمكن أن يسأل جنائيا بالإضافة إلى مسئوليتة المدنية لو سببت معالجته الخاطئة ضرراً لشخص آخر. وقد لخصت المادة الأولى من هذا القانون الأهداف التي توخاها المشرع من وراء اصداره بقولها أن: «المعلوماتية لابد وأن تكون فى خدمة المواطن (....) وانها لا ينبغى لها أن تستخدم كوسيلة للاعتداء على الشخصية الانسانية ولا على حقوق الإنسان ولا على الحياة الخاصة ولا على الحريات الفردية أو العامة». وقد استحدث هذا القانون أنواع من الجرائم يمكن ذكرها فى الآتى: -

أولاً: عدم احترام الشكليات اللازمة والسابقة على معالجة المعلومات الأسمية.

ثانياً: جمع المعلومات الأسمية والاحتفاظ بها بصورة غير شرعية.

ثالثاً: انشاء المعلومات الأسمية.

في المرحلة الثانية: لاحظ المشرع استفحال ظاهرة الاجرام المعلوماتى، ولذلك كان لابد من التدخل ثانية لتضمين قانون العقوبات نصوص جديدة من شأنها مواجهة هذه الظاهرة. ولهذا الغرض تم التفكير فى تقديم مشروع لتعديل قانون العقوبات وقدم هذا المشروع بالفعل إلى البرلمان الفرنسى تحت عنوان

---

(١) انظر فيما يتعلق بهذا القانون:

- Jean Pradel. Les infractions relatives a l'informatique. Revue intérnationle du droit comparé (R.I.D.C.) 1990, pp. 817 et SS.

«الجرائم فى مواد المعلوماتية «أو" Les infractions en matiére informatique»،

ولكن لم يتم «اعتماد هذا المشروع رغم بقاء الحاجة لمواجهة ظاهرة تضخم الإجرام المعلوماتى، غير أنه فى شهر أغسطس ١٩٨٦ تقدم النائب Jaques God-frain باقتراح بقانون تم بالفعل اعتماده بواسطة البرلمان الفرنسى، وصدر به قانون ٥ يناير ١٩٨٨ الذى تم ادماجه فى قانون العقوبات الفرنسي وخصص له الفصل الثانى (المواد من ٤٦٢/٢ إلى ٤٦٢/٩) تحت عنوان «بعض الجرائم فى مواد المعلوماتية «أو" De certaines infraction en matiére informatique" والجدير بالذكر أن الفصل المخصص لهذه الجرائم تم الحاقه بالباب المخصص للجنايات والجميع ضد الأشخاص "Crimes et delits contre Les particuliers" وبالتحديد بعد الفصل الثانى من هذا الباب والمخصص للجنايات والجنح ضد الملكية "Crimes et delits Contre les Propriétés"(١).

هذا وقد ركزت اللجنة التشريعية على فكرة كون الهدف من النصوص الجديدة هو ردع الدخول غير المشروع على برامج المعلوماتية وذلك باعتبارها الهدف الذى توخاه اقتراح النائب Godfrain وهو «حماية النظام المعلوماتى ذاته ضد أى اعتداء خارجى» فهذه الجريمة تعد بحق التجريم الأساسى الذى أتى به النص(٢).

وفى قانون ١٩٨٨ احتلت هذه الجريمة مكاناً أساسياً. ويمكن القول بأنه اذا طرحنا جانباً مسألة تزوير الوثائق المعلوماتية فأن جرائم المعلوماتية تنبثق عن

---

(١) فيما يتعلق بهذا القانون انظر:

- J Deveze, Commentire de la loi No 88/19 du 5 Janvier 1988 relative a la fraude informatique, lamy droit de l'informatique, 1989.
- Jean Pradel: Op. Cit., p. 821.

ولمزيد من التفاصيل حول الجرائم التى استحداثها هذا القانون انظر:

- Jerome Huet et Herbert maisl, droit de l'informtique et des telecommunication paris, 1992, pp. 846 et SS.

(2) Rapport de M. André, Assemblée Nationale, 1986-87 No, 744 p: 12.

(تدور حول) جريمة الدخول غير المشروع إلى نظم المعلوماتية -"Laccés fraudu-leux" أو البقاء فيها. وبتجريم هذا الفعل يمكن القول بأن هذا القانون قد لبى حاجة ملحة جداً بتقديمه الحماية اللازمة(١)،(*).

ونظراً لأهمية قانون ٥ يناير ١٩٨٨ الخاص بجرائم المعلوماتية فسوف نعرض فيما يلي لأهم ما جاء به من أحكام، علماً بأن هذه المواد قد تم تعديلها جزئياً في عام ١٩٩٤ كما تم نقلها ضمن أحكام أخرى من قانون العقوبات بعد تعديله.

مادة وحيدة: يضاف إلى الباب الثاني من قانون العقوبات، بعد الفصل الثاني، فصلا نصه كالتالي:

مادة ٤٦٢/٢:

«يعاقب بالحبس من شهرين إلى سنة وبغرامة تتراوح من ٢٠٠٠ إلى ٥٠٠٠٠ فرنك أو بإحدى هاتين العقوبتين كل من دخل أو مكث غدراً في نظام للمعالجة الآلية للمعلومات أو من جزء منه.

---

(١) انظر في هذا المعنى:

- J- P Buffielan, les Nouveaux delits informatiques, expertises, N°. 1.4 mars 1988, p. 52.
- A Rossion, entrtien a la Révue de l'informatique et des télécom 1988 N°, 2.

(*) على العكس من ذلك، ورغم أن مقرر الجمعية الوطنية كان قد لفت النظر إلى أنه «لابد من أن يقع تحت طائلة العقاب أولئك الذين يبحثون عن الحصول على المعلومات. عن طريق احدى الشبكات المعلوماتية لحظة عملها دون أن يكون لهم الحق في ذلك» فان قانون ١٩٨٨ لم يوفر آية حماية للاتصالات السلكية واللاسلكية Telecommunications. يبدو اذن أن هذا القانون يعاقب أساساً على الأعمال العدوانية Les actes d'agression المادية في هذا المجال مثل الاستيلاء أو التلاعب العدواني لتعطيل نظم المعلوماتية المراد حمايتها. وما يدل على ذلك هو أن استئثار المعلومات أو تحويرها لا يعاقب عليه. وكأن واضعي القانون أرادو ألا يفرضوا أي حماية للمعلومة ذاتها.

- Rapport de M. Andre, op, cit., p. 13.
- Loi du 5 janvier 1988 ralative a la fraude informatique.

وفى حالة ما اذا نتج عن ذلك الغاء أو تعديل المعلومات التى يحتويها ذلك النظام كاتلاف عمله، فإن العقوبة تكون الحبس من شهرين إلى عامين، والغرامة من ١٠ آلاف إلى ١٠٠ ألف فرنك».

**مادة ٣/٤٦٢:**

«يعاقب بالحبس لمدة تتراوح من ثلاثة أشهر إلى ثلاثة أعوام وبالغرامة من ١٠ آلاف إلى ١٠٠ ألف فرنك أو باحدى هاتين العقوبتين. كل من أضر أو زييف بطريقة عمدية وأضراراً بحقوق الغير نظام المعالجة الألية للمعلومات.

**مادة ٤/٤٦٢:**

«يعاقب بالحبس لمدة تتراوح من ثلاثة أشهر إلى ثلاثة أعوام وبالغرامة من ٢٠ ألف إلى ٥٠٠ ألف فرنك أو بإحدى هاتين العقوبتين كل من قام عمداً بطريقة مباشرة أو غير مباشرة واضراراً بحقوق الغير، بادخال معلومات الى نظام معلوماتى معين أو تعديل أو الغاء بث المعلومات التى يحتويها».

**مادة ٥/٤٦٢:**

«يعاقب بالحبس لمدة تتراوح من عام إلى خمسة أعوام وبغرامة يتراوح مقدارها من ٢٠ ألف إلى ٢ مليون فرنك من قام بتزييف وثائق معلوماتية مهما كان شكلها أو طبيعتها، وذلك للاضرار بالغير».

**مادة ٦/٤٦٢:**

«يعاقب بالحبس من عام إلى خمسة أعوام وبغرامة يتراوح قدرها من ٢٠ ألف إلى ٢ مليون فرنك، أو بإحدى هاتين العقوبتين كل من قام عمداً باستخدام الوثائق المعلوماتية المشار إليها فى المادة ٥/٤٦٢».

**مادة ٧/٤٦٢:**

«يعاقب على الشروع فى الجرائم المنصوص عليها فى المواد ٢/٤٦٢ إلى ٦/٤٦٢ بنفس عقوبات الجرائم نفسها».

مادة ٤٦٢/٨:

«كل من شارك فى جمعية أو كان عضواً فى اتفاق يهدف إلى التحضير لإرتكاب فعل أو عدة أفعال مادية لجريمة أو عدة جرائم من تلك المنصوص عليها فى المواد من ٤٦٢/٢ إلى ٤٦٢/٦ يعاقب بالعقوبات المقررة لهذه الجرائم أو بالعقوبة المقررة لأخطر هذه الجرائم».

مادة ٤٦٢/٩:

«يمكن للمحكمة أن تأمر بمصادرة المواد المتعلقة بالجانى والتى تكون قد استخدمت فى ارتكاب الجرائم المنصوص عليها فى هذا الفصل».

وعلى ذلك يكون هذا القانون قد احتوى على عدة أنواع من الجرائم يمكن تقسيمها إلى ثلاث طوائف رئيسية:

**الطائفة الأولى:** تشمل ثلاثة أنواع من الجرائم تضمنتها المواد من ٤٦٢/٢ إلى ٤٦٢/٤ من قانون العقوبات وتهدف هذه الجرائم إلى حماية نظم المعلوماتية ذاتها وتشتمل هذه الطائفة بدورها على ثلاث جرائم مختلفة: -

١- الدخول أو البقاء غير المشروع داخل نظام المعلوماتية.

"Accés ou Maintien Frauduleux"

٢- الاعتداء على سير نظام المعلوماتية.

"Atteinte Portée au fonctionnement d'un systéme"

٣- ادخال معلومات بصورة غير مشروعة فى نظام المعلوماتية أو اتلاف المعلومات الموجودة فيه.

"Intrséléction ou altération de données ou atteinte a leur transmission"

**أما الطائفة الثانية:** فتشمل نوعان من الجرائم تكلمت عنها المواد ٤٦٢/٥ و ٤٦٢/٦ من قانون العقوبات المضافة بقانون ٥ يناير ١٩٨٨ وهاتين الجريمتين هما: -

١ – تزوير الوثائق المعالجة معلوماتياً.

"Falsificauon des documents informatisés"

٢– استخدام الوثائق المعالجة معلوماتياً المزورة.

"Usage des documents informatisés falcifiés"

وعن الطائفة الثالثة: فهى تشمل على عقوبتان تهدفان الى الردع وتغليظ العقاب فى المقام الأول، ونصت عليهما المواد من ٤٦٢/٧ إلى ٤٦٢/٩ وهما: –

١– عقوبة الشروع فى الجرائم السابقة، والتى تهدف إلى ردع النشاط الإجرامى لعصابات المعلوماتية.

٢– عقوبة مصادرة الأدوات المستخدمة فى الجريمة، أو المتحصلة عنها.

- في المرحلة الثالثة:

تمثل اهتمام المشرع الفرنسى بالإجرام المعلوماتى، فى الرغبة فى تعديل قانون العقوبات الفرنسى، وتضمينه أحكام جديدة للحد من هذا النوع من الجرائم. فقد تم تعديل قانون العقوبات الفرنسى فى عام ١٩٩٤ تحقيقاً لهذا الغرض(١).

وكان من مقتضى هذا التعديل اضافة فصلاً ثالثاً للباب الثانى من القسم الثالث من قانون العقوبات. وقد تمت تسمية هذا ا لفصل الثالث «الاعتداءات على نظم المعالجة الألية للمعلومات». ويتكون من المواد ١/٣٢٣ إلى ٧/٣٢٣.

---

(١) حول هذا التعديل، أنظر:

- R Gassin. informatique (fraude informatique). D. Chro. 1995, pp. 174 et SS.
- B Fillion, la reception de l'innovation téchnologique en droit pénal, revue de scicnee crim. 1995, pp. 275 et SS.

وتعالج المادة ١/٣٢٣ من قانون العقوبات الجديد مسألة الدخول أو البقاء غير المشروع إلى نظام المعالجة الآلية للمعلومات(*).

"Accés ou mantien frauduleux dans un système de traitement automatisé de données".

أما المادة ٢/٣٢٣ من قانون العقوبات الجديد فتعالج الاعتداءات الإرادية على سير نظام المعالجة الآلية للمعلومات بحيث يترتب على ذلك تعطيل سير النظام أو اعاقته. والعقوبة التى أقرتها هذه المادة عن الأفعال من هذا القبيل هى السجن لمدة ثلاث سنوات والغرامة التى تصل إلى ٣٠٠ ألف فرنك فرنسى، وهذه المادة عبارة عن ترديد لمحتوى المادة ٣/٤٦٢ من قانون العقوبات القديم.

والمادة ٣/٣٢٣ من قانون العقوبات الجديد تعالج الاعتداءات الموجودة داخل نظام المعالجة الآلية Données على البيانات للمعلومات. والعقوبات التى قررتها هذه المادة لهذا النوع من الأفعال هى نفس العقوبات المقررة عن الأفعال المنصوص عليها فى المادة ٢.٣٢٣ سالفة الذكر. وهذه العقوبات هى عبارة عن السجن لمدة ٣ سنوات والغرامة التى تصل إلى ٣٠٠ ألف فرنك فرنسى. أما الشروع فى ارتكاب هذا النوع من الجرائم فقد نصت عليه المادة ٧/٣٢٣ من قانون العقوبات الجديد والتى تعاقب على الشروع بنفس هذه العقوبات.

هذا وتعالج المادة ٤/٣٢٣ من قانون العقوبات الجديدة، الأفعال الصادرة عن عصابات ا لإجرام المعلوماتى Associations de malfaiteurs فى حالة لو كانت

(*) والملاحظ أن هذه المادة ليست سوى ترديد للمادة ٢/٤٦٢ التى كانت قد تمت اضافتها بقانون ٥ يناير ١٩٨٨ إلى قانون العقوبات القديم، غير أن العقوبات التى أتت بها المادة ١/٣٢٣ مختلفة بعض الشئ. فهى تعاقب على الدخول أو البقاء غير المشروع فى أحد نظم المعالجة الآلية للمعلومات بعقوبة تتمثل فى الحبس لمدة عام وبغرامة لا تزيد عن ١٠٠ ألف فرنك فرنسى. وفى حالة لو ترتب على واقعة الدخول أو البقاء غير المشروع تعديل أو الغاء أو اتلاف للبرامج أو لنظام المعالجة فان العقوبة تتضاعف إلى الحبس لمدة عامين والغرامة التى تصل إلى ٢٠٠ ألف فرنك فرنسى.

هذه الأفعال تشكل واحدة أو أكثر من الجرائم المنصوص عليها في المواد من ١/٣٢٣ إلى ٣/٣٢٣ سالفة الذكر. والعقوبة المنصوص عليها في هذه المادة هي العقوبة أو أشد العقوبات المقررة للفعل ذاته في المواد السابقة Falcification des documents .

أما تزوير الوثائق معلوماتياً فقد عالجته المادة ١/٤٤١ من قانون العقوبات الجديد Informatisés والوثائق المعالجة معلوماتياً في معنى هذه المادة يقصد بها، الشرائط .. Disques وشرائط الكمبيوتر Bandes Magnetiques الممغنطه ... الخ، وهذه المادة يعمل بها جنباً إلى جنب مع المادة ٥/٤٦٢ وتتعلق بتزوير الوثائق المعالجة معلوماتياً أيضاً[١] .

بالإضافة إلي ذلك فقد نصت المادة ٥/٣٢٣ في سبع بنود منها على مجموعة من العقوبات التكميلية بالإضافة إلى العقوبات الأصلية السابقة الذكر.

وتتراوح هذه العقوبات، وهي كثيرة، بين الحرمان من الحقوق المدنية والسياسية ونشر القرار الصادر بالإدانة في الجرائد والأماكن المعدة للنشر.

## الفرع الثاني

## النصوص القانونية المطبقة علي جرائم المعلوماتية

## في التشريع الوطني

سبق أن أوضحنا عند الحديث عن القواعد المطبقة على جرائم المعلوماتية في فرنسا، أن المشرع الفرنسي قد تنبأ بخطورة الاجرام المعلوماتي، وكان من نتائج ذلك أن احتوى قانون العقوبات الفرنسي على مجموعة شبه متجانسة من القواعد القانونية الخاصة بالجرائم المعلوماتية، وتوجد هذه القواعد في قانون

---

(١) انظر ما سبق بشأن المادة ٥/٤٦٢ من قانون العقوبات الفرنسي.

العقوبات الذى تم تعديله فى عام ١٩٩٤ لهذا الغرض كما توجد بعض هذه القواعد فى نصوص لائحيه متفرقة.

أما فى القانون المصرى، فلا يوجد نظام قانونى خاص بحكم جرائم المعلوماتية، وظلت هذه الجرائم، مع ازدياد أهمية الأحساس بها فى القانون المصرى، متروكة لاجتهاد الفقه والقضاء اللذان حاولا عن طريق القياس تبرير تطبيق القواعد الجنائية والإجرائية الخاصة بالجرائم العادية على جرائم المعلوماتية.

والواقع أن القواعد القانونية التى يحاول الفقه والقضاء فى مصر تطويعها لكى تنطبق على جرائم المعلوماتية يمكن تقسيمها الى طائفتين: –

**الطائفة الأولي:** تشمل مجموعة من القواعد الموجودة خارج اطار قانون العقوبات ولكنها تفرض نوع من الحماية الجنائية ضد أفعال شبيه بالأفعال المكونه للجريمة المعلوماتية، ونقصد بتلك القواعد الخاصة بغرض الحماية الجنائية لحقوق المؤلف وما يتشابه معه من الحقوق الذهنية عموماً.

**أما الطائفة الثانية:** فتشمل مجموعة القواعد التى يحتويها قانون العقوبات والخاصة بالسرقة، وخيانة الأمانة وافشاء الأسرار والاتلاف العمدى وغير ذلك من الأفعال التى قد ترتكب ضد نظم المعلوماتية وبرامج الحاسب الآلى.

وفيما يلى سوف نعرض لهاتين الطائفتين من القواعد[1] : –

**الطائفة الأولي: القواعد الموجودة خارج اطار قانون العقوبات:**

توجد مجموعة من القواعد التى يمكن اللجوء إليها فى حسم المشاكل،التى تنشأ عن الجرائم الموجهة ضد نظم وبرامج المعلوماتية،وهذه القواعد توجد كما سبق وأسلفنا خارج قانون العقوبات وان كانت تتصف بأنها تفرض نوع من

---

(١) د/ أحمد حسام طه تمام – المرجع السابق – ص ٩٢ وما بعدها.

العقوبات الجنائية على مخالفة أحكامها. وهذه القواعد تتصل أساساً بالحماية الجنائية التى قررها المشرع للحفاظ على الحقوق الذهنية، وذلك عن طريق اعتماد نصوص مصرية خالصة لهذا الغرض كما هو الحال بالنسبة للقوانين المصرية المتعلقة بحماية الملكية الفكرية والأدبية، وحماية الملكية الصناعية وكذلك حماية براءات الاختراع والرسوم والنماذج الصناعية.

والحماية الجنائية لمجموع هذه الحقوق لاتتقرر عن طريق نصوص داخلية فقط، ولكن قد تفرضها اتفاقيات دولية نافذة فى مصر، وينبغى على المشرع المصرى أن يلتزم بفرض الحماية التى تقررها فى القانون الداخلى شأنها فى ذلك شأن القواعد الوطنية(*).

**أولاً: القوانين المتعلقة بحماية الملكية الذهنية:**

من المعلوم أن الحق قد يكون مالياً، وقد يكون غير مالى ولكن إلى جانب

---

(*) من المعروف أنه على المستوى الدولى،تتعدد الاتفاقيات التى تهتم بحماية حقوق الملكية الصناعية، وكذلك بحماية حقوق المؤلفين.

- فيما يتعلق بالملكية الصناعية، عقدت اتفاقية باريس المبرمة فى ٢٠ مارس ١٨٨٣ والخاصة بحماية الملكية الصناعية فى كافة نواحيها، وكذلك اتفاقية مدريد المبرمة فى ١٤ ابريل ١٨٩١ والخاصة بوضع نظام دولى لتسجيل العلامات والبيانات التجارية. وأيضاً أبرمت اتفاقية ٦ نوفمبر ١٩٢٥ والخاصة بوضع نظام دولى لتشغيل الرسم والنماذج الصناعية.

أما بالنسبة للاتفاقيات الدولية فى شأن حقوق المؤلف فمن أهمها اتفاقية برن FERN التى أبرمت فى ٩ سبتمبر ١٨٨٦ والخاصة بحماية حقوق المؤلف. وقد عدلت هذه الاتفاقية عدة مرات بهدف توسيع نطاق الحماية بجعلها مسايرة للتطور الحديث فى وسائل النشر، فتم تعديلها فى مؤتمر باريس عام ١٨٩٦، ثم فى مؤتمر برلين عام ١٩٠٨ وفى مؤتمر روما فى عام ١٩٢٨، ثم فى مؤتمر بروكسيل فى ٢٦ يونيو ١٩٤٨. ثم قامت منظمة اليونسكو التابعة للأمم المتحدة بتنظيم عقد اتفاقية جنيف الخاصة بحماية حقوق المؤلف فى ٦ سبتمبر ١٩٥٢. وتعتبر مصر طرفاً فى الاتفاقيات الدولية النافذة حالياً.

لمزيد من التفاصيل، انظر: د/ إبراهيم أحمد إبراهيم، الحماية الدولية لحق المؤلف – القاهرة – ١٩٩٢.

هذين النوعين من الحقوق، يوجد نوع ثالث يجمع بين صفات النوعين السابقين النوع المالي والنوع غير مالي. وهذا النوع الثالث يطلق عليه الحقوق الذهنية Droits Intellectuels وبشأن هذه الحقوق تنص المادة ٨٦ من القانون المدني المصري الحالي على أن «الحقوق التي ترد على شئ غير مادي تنظمها قوانين خاصة»، والأشياء غير المادية هي التي لا يمكن أن تدرك بالحس المادي بل تدرك بالفكر المجرد(١)، والأمثلة على الحقوق التي ترد على الأشياء غير المادية أو ما يسمى بالملكية الذهنية، عديدة فهناك الملكية الصناعية، وتتمثل في حق الاستئثار الصناعي التي تخول صاحبها أن يستأثر في مواجهة الكافة باستغلال ابتكار جديد أو استخدام علامة مميزة(*).

وإلى جانب الملكية الصناعية توجد الملكية الإدبية والفنية، ويقصد بها حق الشخص على نتاج ذهنه وثمرة فكره، أياً كان المظهر الذي يتخذه هذا الناتج أو تلك الثمرة.

---

(١) انظر بشأن تقسيم الحقوق وموقع الحقوق الذهنية في داخلها:
- د/ عبد المنعم البدراوي – مبادئ القانون – القاهرة – سنة ١٩٧٥، فقرة ٦٩ وما بعدها.
- د/ سليمان مرقص – شرح القانون المدني (المدخل للعلوم القانونية) – القاهرة – سنة ١٩٦٧، ص ٧٤ وما بعدها.

(*) وتتنوع حقوق الملكية الصناعية إلى حقوق ترد على ابتكارات جديدة وهي براءات الاختراع والرسوم والنماذج الصناعية والاسم التجاري.
وقد أصدر المشرع المصري عدة قوانين تكفل حماية الملكية الصناعية. فأصدر القانون رقم ٥٧ لسنة ١٩٣٩ بشأن العلامات والبيانات التجارية، ثم القانون رقم ١٣٢ لسنة ١٩٤٩ الخاص ببراءات الاختراع والرسوم والنماذج الصناعية، ثم القانون رقم ٥٥ لسنة ١٩٥١ بشأن الأسماء التجارية.
وتنص المادة الأولى من القانون رقم ١٣٢ لسنة ١٩٤٩ سالف الذكر، «على أن تمنح براءة الاختراع وفقاً لإحكام هذا القانون عن كل ابتكار جديد قابل للاستغلال الصناعي سواء كان متعلقاً بمنتجات جديدة، أم بطرق أو وسائل صناعية مستحدثة أم بتطبيق جديد لطرق أو وسائل صناعية معروفة.
- ونصت المادة الثانية من القانون على الاختراعات المستبعدة من هذا النظام، أي التي لا يجوز منح براءة اختراع عنها.

وقد ذهب الفقه المصرى إلى أن نصوص قانون براءات الاختراع تنطبق على الجانب المادى من نظام المعالجة الآلية للمعلومات، ولكن مع ملاحظة أن العقوبات التى يحتويها القانون رقم ١٣٢ لسنة ١٩٤٩ والتعديلات التى أدخلت عليه فى عامى ١٩٧٩، ١٩٨١، يجب اعادة النظر فيها بحيث تصبح أكثر ردعاً(١).

أما فيما يتعلق بحق المؤلف، فقد أصدر المشرع القانون رقم ٣٥٤ لسنة ١٩٥٤ بشأن حماية حق المؤلف. ثم تم تعديل المادة ٤٧ من هذا القانون بالقانون رقم ٣٨ الصادر فى عام ١٩٩٢(٢)، وأصبحت هذه المادة تنص بعد تعديلها على أنه:

«يعاقب بالحبس وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه كل من ارتكب أحد الأفعال الآتية»: –

أولاً: من اعتدى على حق من حقوق المؤلف المنصوص عليها فى المواد ٥، ٦، ٧ فى هذا القانون.

ثانياً: من أدخل فى مصر بقصد الاستغلال دون اذن المؤلف أو من يقوم مقامه، مصنفاً منشوراً فى الخارج مما تشمله الحماية الجنائية التى تفرضها أحكام هذا القانون.

ثالثاً: من باع أو عرض للبيع أو للتداول أو للايجار مصنفاً مقلداً مع علمه بتقليده.

رابعاً: من قلد فى مصر مصنفاً منشوراً فى الخارج أو باعه أو عرضه للبيع أو للتداول أو للايجار مع علمه بتقليده.

خامساً: من قلد فى مصر مصنفاً منشوراً فى الخارج أو باعه أو عرضه للبيع،أو للتداول أو للايجار،أو صدره أو شحنه للخارج مع علمه بتقليده.

---

(١) انظر فى ذلك: د/ عمر الفاروق الحسينى، الجرائم المتصلة بالحاسب الآلى وأبعادها الدولية، القاهرة ١٩٩٢، ص ص ١٩ – ٢٠.

(٢) منشور بالجريدة الرسمية، العدد ٢٣ فى ٤ يونية ١٩٩٢.

وتتعدد العقوبات بتعدد المصنفات محل الجريمة . وفي حالة العود تكون العقوبة الحبس والغرامة التى لا تقل عن عشرة آلاف جنيه ولا تزيد على خمسين ألف جنية . وفي جميع الأحوال تقضي المحكمة بمصادر النسخ المقلدة والأدوات المستخدمة في التقليد، وينشر ملخص الحكم الصادر بالإدانة فى جريدة يومية أو أكثر على نفقة المحكوم عليه . «ويجوز للمحكمة عند الحكم بالإدانة أن تقضي باغلاق المنشأة التى استغلها المقلدون أو شركاؤهم فى ارتكاب أحد الأفعال المشار إليها مدة لا تزيد على ستة أشهر» .

ويذهب الفقه المصرى – بحق – إلى أن هذا النص ينطبق على الجرائم الواقعة على حقوق المؤلف المتصلة بالحاسب الآلى، وذلك لأن المشرع عندما عدل أحكام القانون رقم ٣٥٤ لسنة ١٩٥٤ بالقانون رقم ٣٨ لسنة ١٩٩٢ قد أضاف الى المصنفات التى يحميها القانون والمنصوص عليها فى المادة الثانية من القانون رقم ٣٥٤، أضاف إليها . «مصنفات الحاسب الآلى من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الداخلية» . وقيل بأنه حتى قبل اضافة برامج الحاسب الآلى إلى المصنفات المحمية فى عام ١٩٩٢، كان الفقة مستقراً على أنها تدخل ضمن المصنفات التى يحميها القانون، وذلك استناداً إلى نص المادة الأولى من قانون حماية حق المؤلف رقم ٣٥٤ لسنة ١٩٥٤ والتى تنص على أنه «يتمتع بحماية هذا القانون مؤلفوا المصنفات المبتكرة فى الآداب والعلوم والفنون، أياً كان نوع هذه المصنفات أو طريقة التعبير عنها أو أهميتها أو الغرض من تصنيفها» . وكذلك استناداً إلى نص المادة الثانية من القانون رقم ٣٥٤ قبل تعديلها عام ١٩٩٢ والتى كانت تنص على أنه ... «وتشمل هذه الحماية بوجه عام مؤلفى المصنفات التى يكون مظهر التعبير عنها الكتابة أو الصورة أو الرسم أو التصوير أو الحركة» . ويعنى ذلك ان

برامج الحاسب الآلى كانت تدخل ضمن إطار هذا النص الذى صيغ بصورة واسعة تسمح بذلك[1] .

**ثانياً: القانون رقم ١٥ لسنة ٢٠٠٤ بشأن تنظيم التوقيع الالكتروني[1]:**

ويضم القانون ٣٠ مادة، ويعنى بتنظيم التوقيع الإلكترونى، وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات[2]. وكان لصدور هذا القانون صدى واسع فى حسم العديد من المشكلات القانونية، التى كان يتصدى لها القضاء بالاجتهاد، فجاء هذا القانون بتعريفات واضحة ومحددة لماهية المحرر الإلكترونى والوسيط الإلكترونى.

**الطائفة الثانية: القواعد التي يتضمنها قانون العقوبات:**

نظراً لأن الحماية التى تقررها القواعد المنظمة للملكية الفكرية، ليست كافية لمواجهة مد جرائم المعلوماتية وتأثيرها الخطيرة على المصالح الاقتصادية والذهنية، كان لابد من الاتجاه قبلة الحماية الجنائية التى يقررها قانون العقوبات بقسوته المعهوده لكى تنطبق على جرائم المعلوماتية. غير أنه وقت صياغة أحكام قانون العقوبات المصرى لم يكن المشرع المصرى قد تنبأ لخطورة هذا

(١) انظر فى ذلك:
- د/ على عبد القادر القهوجى – مرجع سابق – ص ٨ وما بعدها.
- د/ برهام عطا الله – المصنفات المحمية فى قانون حماية حق المؤلف، منشور فى كتاب حق المؤلف بين الواقع والقانون، صادر عن كلية الحقوق جامعة القاهرة، ١٩٩٩، ص ٤٤ وما بعدها.
- د/ محمد حسام محمود لطفى – الحماية القانونية لبرامج الحاسب الآلى – القاهرة ١٩٧٨، ص ١٥٢ وما بعدها.

(٢) للمزيد من المعلومات بشأن تقرير موقف المشرع بشأن قانون التوقيع الالكترونى المصرى رقم ١٥ لسنة ٢٠٠٥.

براجع: د/ أشرف توفيق شمس الدين – الحماية الجنائية للمستند الالكترونى (دراسة مقارنة) – دار النهضة العربية – سنة ٢٠٠٦ – ص ١٥٣ وما بعدها.

(٣) نشر بالجريدة الرسمية – العدد ١٧ تابع (د) – ٢٢ ابريل ٢٠٠٤.

النوع من الجرائم. كما أنه لم يتم تعديل قانون العقوبات لكى يتلائم مع التطور الحاصل فى هذا المجال.

ولذلك لم يكن هناك بد من الاستعانة بالنصوص المطبقة على الجرائم العادية، لتوفير نوع من الحماية الجنائية لنظم المعلوماتية وما تحتوى عليه من برامج ومعلومات وما إلى ذلك، خصوصاً وأن جرائم المعلوماتية لا تخرج عن كونها إما سرقة أو حيانة أمانة، أو اخفاء، أو تخريب أو اتلاف أو تزوير، مع اختلاف وحيد يتعلق بخصوصية الشئ الواقع عليه هذه الجرائم، رغم أن هناك قاسم مشترك بينها وهى أنها تقع جميعها على مال منقول مملوك للغير باستثناء جريمة التخريب والاتلاف التى يمكن أن تقع على عقار أو منقول(١).

علاوة على ذلك أمكن للفقه والقضاء فى مصر تطويع نصوص قانون العقوبات المصرى بشأن حماية الحياة الخاصة، وكذلك النصوص التى تجرم افشاء الأسرار على بعض الجرائم التى ترتكب ضد أو عن طريق نظم المعلوماتية(٢).

**أولاً: القواعد المتعلقة بحماية حرمة الحياة الخاصة:**

النصوص الواردة فى قانون العقوبات والمتعلقة بحساية حرمه الحياة الخاصة، هى المواد ٣٠٩ مكرر، ٣٠٩ مكرر (أ). وكذلك ٣١٠ عقوبات والتى تجرم افشاء الأسرار. وتنص المادة ٣٠٩ مكرر من قانون العقوبات على أنه: «يعاقب بالحبس مدة لا تزيد على سنة كاملة من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية فى غير الأحوال المصرح بها قانوناً أو بغير رضاء المجنى عليه:

( أ ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه، محادثات جرت فى مكان خاص أو عن طريق التليفون.

---

(١) د/ على عبد القادر القهوجى – المرجع السابق – ص ٤٦ وما بعدها.

(٢) د/ عمر الفاروق الحسينى – المرجع السابق – ص ٤٢ وما بعدها.

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه، صورة شخص فى مكان خاص.

فاذا صدرت الأفعال المشار إليها فى الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين فى ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً.

ويعاقب بالحبس الموظف العام الذى يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفته.

ويحكم فى جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم فى الجريمة، كما يحكم بمحو التسجيلات المتحصلة عنها أو اعدامها.

**- أما المادة ٣٠٩ مكرراً ( أ ) من ذات القانون فتنص على أن:**

«يعاقب بالحبس كل من أذاع أو سهل اذاعة أو استعمل ولو فى غير علانية تسجيلاً أو مستنداً متحصلاً عليه باحدى الطرق المبينة بالمادة السابقة، أو كان ذلك بغير رضاء صاحب الشأن»(*).

ويعاقب بالسجن الموظف العام الذى يرتكب أحد الأفعال المبينة بهذه المادة اعتماداً على سلطة وظيفتة.

ويحكم فى جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم فى الجريمة، أو تحصل عنها، وبمحو التسجيلات المتحصلة عن الجريمة أو اعدامها.

---

(*) ذكر المشرع فى نص المادة ٣٠٩ مكرراً ( أ ) «لفظ سهل إذاعة، أو استعمل، وقد أراد المشرع تجريم فعل الاستعمال المكون للركن المادى لجريمة الاستعمال، والتى يتصور وقوعها فى نطاق المعلوماتية، من استعمال مستنداً أو تسجيلاً تم الحصول عليه المنصوص عليها فى المادة السابقة، وقد كان ذلك بدون أذن ورضاء صاحبه، وقد استعمل بقصد الإضرار وافساد اسرار الغير. وكذلك الموظف العام الذى يكون قد حصل على هذه التسجيلات أو المستندات بحكم الوظيفة وقد قام باستعمالها دون إذن ورضاء صاحبها اضراراً لصاحبها.

وقد قيل بأن هذين النصين قد أتيا بجرائم ثلاث من المتصور حدوثها عن طريق نظم المعلوماتية: -

**الجريمة الأولي:** هى المنصوص عليها بالمادة ٣٠٩ مكرر وهى جريمة الحصول على الحديث أو الصورة بطريق غير مشروع.

**أما الجريمتان الثانية والثالثة:** فقد وردتا فى المادة ٣٠٩ مكرراً (أ)، وهما جريمة اذاعة أو استعمال الحديث أو الصورة، وجريمة التهديد بالاذاعة أو الاستعمال.

وبشأن تجريم افشاء الأسرار وهى جريمة كثيرة الحدوث فى مجال المعلوماتية، فقد نصت المادة ٣١٠ من قانون العقوبات على أنه:

«كل من كان من الأطباء أو الجراحين أو الصيادلة أو القوابل أو غيرهم، مودعاً إليه بمقتضى صناعته أو وظيفته سر خصوص أؤتمن عليه، فافشاه فى غير الأحوال التى يلزم القانون فيها بتبليغ ذلك، يعاقب بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تتجاوز خمسمائة جنية».

ولا تسرى أحكام هذه المادة إلا فى الأحوال التى لم يرخص فيها قانوناً بافشاء أمور معينة كالمقرر فى المواد ٢٠٥، ٢٠٤، ٢٠٣، ٢٠٢ من قانون المرافعات فى المواد المدنية والتجارية.

**ثانياً: القواعد الخاصة بجرائم الاعتداء علي الأموال:**

أما النصوص المتعلقة بجرائم المشار إليها سلفاً والتى قرر الفقه والقضاء المصرى مد نطاق تطبيقها على جرائم المعلوماتية فهى متعدده، وقد أمكن بالفعل تخطى عقبات تطبيقها على جرائم المعلوماتية، وان كان الأمر أحوج إلى تعديل قانون العقوبات المصرى لهذا الغرض.

- وهذه النصوص هي:

١- نصوص قانون العقوبات المتعلقة بتجريم الإتلاف وما فى حكمه، (المواد ٣٦١ ع مصرى وما بعدها).

٢- نصوص قانون العقوبات المتعلقة بجريمة السرقة، (المواد ٣١١ ع مصرى إلى ٣٢٧ ع مصرى).

٣- نصوص قانون العقوبات المتغلقة بجريمة خيانة الأمانة، (المواد ٣٤١ عن مصرى و ٣٤٣ ع مصرى).

٤- نصوص قانون العقوبات المتعلقة بجريمة التزوير، (المواد ٢١١ ع مصرى إلى ٢٢٧ ع مصرى).

٥- نصوص قانون العقوبات المتعلقة التخريب.

٦- نصوص قانون العقوبات المتعلقة بالأخفاء.

## الفرع الثالث

## النصوص القانونية المطبقة علي جرائم المعلوماتية في الدول العربية

• - سلطنة عمان: تضمن التشريع العقابى العمانى النص على عقوبات لغالبية الأفعال غير المشروعة فى مجال استخدامات الحاسب الآلى، حيث جاء بنص المادة ٢٧٥ من قانون العقوبات المعدل بالمرسوم الصادر عام ٢٠٠١م الخاص بجرائم الحاسب الآلى بأن يعاقب بالسجن لمدة لا تقل عن ثلاثة أشهر ولا تزيد على السنتين وبغرامة تتراوح بين مائة ريال عمانى إلى خمس مئة ريال أو بإحدى هاتين العقوبتين لكل من تعمد استخدام الحاسب الآلى فى ارتكاب الأفعال الآتية(*):

(*) راجع النص الكامل للقانون على موقع وزارة العدل العمانية..

- http //. www. moj. gov.

أ - الالتقاط غير المشروع للمعلومات أو البيانات.

ب- الدخول غير المشروع على أنظمة الحاسب الآلى.

جـ- التجسس والتنصت على البيانات والمعلومات.

د - انتهاك خصوصيات الغير أو التعدى على حقهم فى الاحتفاظ بأسرارهم وتزوير البيانات أو الوثائق المبرمجة.

هـ- إتلاف وتغيير ومحو البيانات والمعلومات.

و - جمع البيانات والمعلومات وإعادة استخدامها.

ز - التعدى على برامج الحاسب الآلى سواء بالتعديل أو الاصطناع.

حـ- نشر واستخدام برامج الحاسب الآلى بما يشكل انتهاكاً لقوانين حقوق الملكية والأسرار التجارية.

- قطر: أيضاً ،وشأن سلطة عمان، تضمن التشريع العقابى القطرى النص على عقوبات رادعة لمرتكبى جرائم الحاسب الآلى وذلك حيث جاء الفصل الخامس من الكتاب الثالث من قانون العقوبات المعدل بالقانون رقم ١١ لسنة ٢٠٠٤ بعنوان جرائم الحاسب الآلى فى المواد من ٣٧٠ إلى ٣٨٠ بتجريم العديد من الأفعال غير المشروعة المصاحبة لاستخدامات الحاسب الآلى، حيث تنص المادة ٣٧٩ على أنه يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، كل من استخدم حاسباً آلياً بطريق التلاعب، سواء عن طريق إدخال معلومات، أو بيانات زائفة أو غير حقيقية، أو عن طريق العبث بالبرامج وهذه المادة يمكن أن تنطبق على كافة أفعال التصيد الاحتيالى لأرقام وبيانات بطاقات الدفع الإلكترونى.

وتنص المادة ٣٨٠ على أنه يعاقب بالحبس مدة لا تتجاوز ٥ سنوات، كل شخص ارتكب تزويراً فى المستندات المعالجة آلياً، أياً كان شكلها، وترتب عليه الإضرار بالغير، أو استعمل هذه المستندات المزورة مع علمه بذلك.

ويعد تزويراً فى برامج الحاسب الآلى أو البرامج المسجلة على ذاكرته للحصول على نتائج غير صحيحة.

- إمـارة دبي: شأن باقى القوانين والتـشريعات العقـابية تطبق المواد المتعلقة بالسرقة والتزوير والاحتيال وخيانة الأمانة، ولا يوجد نصوص صريحة تجـرم هذه الأفعال، إلا أن القـانون رقم ٢ لسنة ٢٠٠٢م بشأن المعاملات والتجارة الإلكترونية قد نص فى المادة ٣٢ من الفصل السابع على أنه مع عدم الإخلال بأية عقوبة أشد ينص عليها أى قانون آخر، يعاقب كل من ارتكب فعلاً يشكل جريمة بموجب التشريعات النافذة، باستخدام وسيلة إليكترونية بالحبس لمدة لا تزيد على ستة أشهر وبغرامة لا تتجاوز ١٠٠,٠٠ درهم أو بإحدى هاتين العقوبتين، ويعاقب بالعقوبة الأشد إذا كانت العقوبات المقررة فى تلك التشريعات تزيد على العقوبة المقررة فى هذه المادة.
- المغـرب: شأن معظم القوانين العقابية العربية، خلا أيضاً القانون الجنائى المغربى من أية نصوص واضحة وصريحة تجرم هذه الأفعال، إلا أن الباب العاشر منه تضمن تعديلاً بتاريخ ١١ نوفمبر عام ٢٠٠٣م، بإضافة الفصول المتضمنة «المواد ٦٠٧/٣ حتى ٦٠٧/١١» لتجريم كافة الأفعال غير المشروعة، المتعلقة بنظم المعالجة الآلية للمعلومات وذلك على النحو التالى:

أ – الفصل ٦٠٧/٣ يعاقب بالحبس من شهر إلى ثلاثة أشهر وبالغرامة من ٢,٠٠٠ إلى ١٠,٠٠٠ درهم أو بإحدى هاتين العقوبتين فقط كل من دخل إلى مجموع أو بعض نظام للمعالجة الآلية للمعطيات عن طرق الاحتيال. ويعاقب بالعقوبة نفسها من بقى فى نظام للمعالجة الآلية للمعطيات أو فى جزء منه كان قد دخله عن طريق الخطأ وهو غير مخول له حق دخوله، وتضاعف العقوبة إذا نتج عن ذلك حذف أو تغيير للمعطيات المدرجة فى نظام للمعالجة الآلية للمعطيات أو اضطراب فى سيره.

ب– الفصل ٦٠٧/٤ دون الإخلال بالمقتضيات الجنائية الأشد يعاقب بالحبس من ستة أشهر إلى سنتين وبالغرامة من ١٠,٠٠٠ إلى

١٠٠,٠٠٠ درهم كل من ارتكب الأفعال المشار إليها فى الفصل السابق، فى حق مجموع أو بعض نظام للمعالجة الآلية للمعطيات تبين أنه يتضمن معلومات تخص الأمن الداخلى أو الخارجى للدولة، أو أسراراً تهم الاقتصاد الوطنى، دون الإخلال بالمقتضيات الجنائية الأشد، وترفع العقوبة إلى الحبس من سنتين إلى خمس سنوات وبالغرامة من ١٠٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم إذا نتج عن الأفعال المعاقب عليها فى الفقرة الأولى من هذا الفصل، تغيير المعطيات المدرجة فى نظام للمعالجة الآلية للمعطيات أو حذفها أو اضطراب فى سير النظام، أو إذا ارتكبت الأفعال من طرف موظف أو مستخدم أثناء مزاولة مهامه أو بسببها، أو إذا سهل للغير القيام بها.

جـ- الفصل ٦٠٧/٥ يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من ١٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم أو بإحدى هاتين العقوبتين، كل من عرقل عمداً سير نظام للمعالجة الآلية للمعطيات، أو أحدث فيه خللاً.

د - الفصل ٦٠٧/٦ يعاقب بالحبس من سنة إلى ثلاث سنوات وبالغرامة من ١٠,٠٠٠ إلى ٢٠٠,٠٠٠ درهم أو بإحدى هاتين العقوبتين فقط، كل من أدخل معطيات فى نظام للمعالجة الآلية للمعطيات، أو أتلفها أو حذفها منه أو غير المعطيات المدرجة فيه، أو غير طريقة معالجتها أو طريقة إرسالها عن طريق الاحتيال.

هـ- الفصل ٦٠٧/٧ دون الإخلال بالمقتضات الجنائية الأشد، يعاقب بالحبس من سنة إلى خمس سنوات وبالغرامة من ١٠,٠٠٠ إلى ١,٠٠٠,٠٠٠ درهم كل من زور أو زيف وثائق المعلومات أيا كان شكلها، إذا كان من شأن التزوير أو التزييف إلحاق ضرر بالغير. دون الإخلال بالمتقضيات الجنائية الأشد تطبق العقوبة نفسها، على كل من استعمل وثائق المعلومات المشار إليها فى الفقرة السابقة وهو يعلم أنها مزورة أو مزيفة.

# الفصل الثالث

## الجريمة المعلوماتية فى الإتفاقيات الدولية

- المبحث الأول : الجريمة المعلوماتية فى إتفاقية بودابست ٢٠٠١ .
- المبحث الثانى : إتفاقية الجرائم المعلوماتية (المجلس الأوروبى).

## الفصل الثالث

## الجريمة المعلوماتية فى الإتفاقيات الدولية

لقد مهدت الثورة الصناعية التى تفجرت فى منتصف القرن التاسع عشر ، لبزوغ ثورة جديدة هى ثورة المعلومات (1) ، التى تقترن دائمًا بفكرة الحاسب ، التى بدأها charles babbage الذى يعتبر أول من فكر فى الحاسب الرقمى (Digital Computer) من خلال سعيه الدؤوب لميكنة (مكننة) بعض العمليات الحسابية Mechanisation of Arithmatics حيث اكتشف آلة الفروق ثم الآلة التحليلية ، وفى سنة ١٩٤٣ قام جون فان نيومن J. M. Neumann عالم الرياضيات الأمريكى بوضع أسس الحاسب كما هو معروف الآن، والذى يتكون من خمسة مكونات (*) ، فظهر الحاسب كجهاز رئيسى فى الإعلام الآلى أو المعلوماتية (2) ، وبفضل الحاسب يعيش العالم الآن عصر المعلومات الذى يتسم بالتطور السريع لتكنولوجيا الحاسبات (3) ، حيث أخذت المعلومات الآن فى التزايد والتفاعل مع التقدم العلمى والتطور التكنولوجى ، كل دقيقة بل كل ثانية ، وبات تدفق المعلومات أساساً للرقى الحضارى للدول ، وبسبب انفجار المعلومات

---

(1) د/ على عبد القادر القهوجى – الحماية الجنائية لبرامج الحاسب الآلى – مجلة الحقوق للبحوث القانونية والاقتصادية – كلية الحقوق – جامعة الإسكندرية – سنة ١٩٩٢ – ص٢٦٦ .

(*) أهم هذه المكونات اثنتان هما وحدة المعالجة المركزية central processing unit التى يتم بواسطتها تنفيذ سلسلة العمليات الحسابية والمنطقية المطلوب تنفيذها ، والذاكرة Memory التى يتم فيها حفظ نتيجة كل عملية حيث يتم تنفيذ العملية طبقاً لمجموعة من التعليمات Instruc-tions أو البرامج programms المختزنة أيضاً فى الذاكرة .

يراجع ص من هذا المؤلف بشأن مكونات الحاسب الآلى .

(2) د/ عبد الحميد عبدونى – استعمالات الحاسوب فى التقويم النفسى وإتخاذ القرارات – مجلة العلوم الاجتماعية والإنسانية – جامعة باتنة – الجزائر – العدد الثانى – ديسمبر ١٩٩٤ – ص١٠٩ .

(3) لواء د/ علاء الدين محمد فهمى – إتجاهات التطور العالمى لتكنولوجيا المعلومات – بحث مقدم لندوة المعلوماتية والقانون – كلية الحقوق – جامعة الإسكندرية – فبراير ١٩٩٤ – ص١ .

Informatique Explosion – إن صح هذا التعبير – وتزايدها ، بدأت الدول تهتم بأساليب جمع المعلومات وتبويبها وتصنيفها وتحليلها بنية الإفادة منها .

في ذات الوقت الذى تطورت فيه المستحدثات التقنية (التكنولوجية) المتقدمة، والتى استهدفت التحكم فى هذه المعلومات وتخزينها واسترجاعها ، وهو ما يعرف بتكنولوجيا المعلومات Information tecknology أو المعلوماتية Informatique ، وباتت وفرة المعلومات معياراً لجدوى جهود التنمية وزيادة الإنتاج ورسم السياسات ، واتخاذ أنجح القرارات للنهوض باقتصاد الأمم ، فالمعلومات –ولا شئ غيرها– هى أساس السيادة الاقتصادية للدول التى تملكها ، ولا غرو فإن ما أنتجه العقل البشرى فى الخمسين سنة السابقة على عام ١٩٨٤ يعادل ستة أمثال ما أنتجه العقل البشرى فى خمسة قرون سابقة [1]. ولا مراء فى أن السنوات العشر الأخيرة قد تحقق فيها أكثر مما تحقق منذ منتصف القرن العشرين حتى بداية القرن الحادى والعشرين، وباستخدام تكنولوجيا المعلومات وبرامج الحاسب، يمكن أن يتحقق إنجازات علمية وتقنية فى عام واحد ما يعادل أو يكاد يفوق ما تحقق خلال فترات زمنية طويلة من تقدم وتطور خطت به الإنسانية عصور مضت .

وإزاء إفراز العقول البشرية لهذا الكم الهائل من المعلومات ، أصبح من المستحيل حفظ هذه المعلومات واسترجاعها بكفاءة ، وكان لابد من استخدام الحاسبات فى هذا الصدد ، وقد تم ذلك فعلاً، ولكن فى ظل بيئة المعلومات المخزنة أليًا كان لابد أن (تضعف) [2] قبضة الأمن والمراقبة والتحكم، وأن تزدهر عمليات

---

(١) د/ شعبان عبد العزيز خليفة – شبكة المعلومات (دراسة فى الحاجة والهدف والأداء) – مجلة المكتبات والمعلومات العربية – دار المريخ للنشر – السنة الرابعة – العدد الثانى – ابريل ١٩٨٤– ص١٢ .

(٢) د/ هشام محمد فريد رستم – قانون العقوبات ومخاطر تقنية المعلومات – مرجع سابق– ص٨.
وقد أشار محمد محمد شتا إلى أنه تم التصرف فى صياغة العبارة لإحكام الجانب اللغوى دون تعرض لمحتواها العلمى الدقيق .
يراجع : محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلى – مرجع سابق – ص٦٨ .

التجسس على المعلومات المعالجة الكترونيًا وسرقتها، حتى باتت تشكل تهديداً بالغًا لسائر المنظمات الحكومية والخاصة ، التى تعتمد أعمالها على الحاسبات والشبكات الاتصالية ، وترتفع مخاطر إساءة استخدام الحاسبات والتلاعب فى البرامج وملفات المعلومات المخزنة أليًا ، بقصد الحصول على أموال وأصول وخدمات غير مستحقة ، وتهيئ حرية النسخ للبرامج وتداولها عن غير طريق منتجها الأصلى مجالاً واسعًا لدى الفيروسات المعلوماتية التى تتفشى، وتصيب الأنظمة والشبكات بأنواع ودرجات من العطب والضرر مختلفة، وتبرز كأهداف لعمليات التخريب والإرهاب – المنظم – منظومة معالجة المعلومات وقواعد البيانات وبرامج الحاسبات وشبكات الاتصال ، لاسيما المستخدم منها فى الأغراض الدفاعية (١) .

وبدأت الدول المتقدمة كالولايات المتحدة الأمريكية تعانى من جرائم العبث والتخريب الموجه إلى الحاسبات ذاتها ، وسرقة المعلومات المخزنة فيها والاحتيال والغش المالى المرتبط بها . والاستخدام غير المصرح به لخدمات الحاسبات وغيرها من الجرائم الفنية Technocrimes التى تحولت من مجرد انتهاكات فردية لأمن النظم إلى ظاهرة تقنية Technological Phenomenon تهدد الأمن القومى قبل أن تهدد الشركات والمؤسسات والأفراد.(٢) ، لاسيما وأن شبكات الاتصال تيسر ارتكاب هذه الجرائم عبر الحدود ، بحيث أنه يمكن لشخص تتوافر لديه الدراية الفنية ، ويتسلح ببعض التجهيزات التقنية ، أن يمحوا أو يعدل أو يخرب أو يستولى على بيانات معالجة الكترونياً فى دولة أخرى خلال ثوان محدودة (٣) .

---

(١) المرجع ذاته .

(2) Nonn B. Parken, crime by computer, vharles scribner's sons, New York, 1976, p. 34 .

(3) Stein schjolberg, computers and penal legislation a study of the legal politics of a new technology, oslo univer, 1983, p.p.9-10.

مشار إليه لدى د/ هشام محمد فريد رستم – المرجع السابق – ص١٠ .

ويزداد الأمر خطورة عندما يتعلق بالاعتداء على البرامج التى تتضمن خطط دفاعية أو هجومية تخص دولة، أو أنظمة الإنتاج الحربى أو الاقتصادى، أو برامج تطوير صناعة معينة، أو دراسات مبدئية لإنتاج أدوية وخاصة الأدوية الاستراتيجية وذلك على المستوى الوطنى ، أو يكون الاعتداء على برامج تختزن أنظمة شركات خاصة ودراسات تطوير مشروعات استثمارية ، أو أنظمة العمل فى القطاع الاقتصادى (يشمل البنوك والبورصة) ، أو مراحل إنتاج سلعة، أو ما إلى ذلك من الأمور التقنية والذهنية التى اعتبرت اتفاقية Trips – ومن بعدها اتفاقية بودابست 2001 – البرامج فيها بمثابة مؤلفات تستحق الحماية كأى مؤلف تقليدى أخر، مع مراعاة الفارق فى المضمون والفن Technique . وما إلى غير ذلك من عوامل التمايز – والاختلاف – بين المصنفات بمفهومها التقليدى ، والمصنفات بمفهومها الحديث .

وتصل صعوبة الأمر إلى مدى متقدم عندما تتعلق بجرائم ذات طبيعة خاصة متميزة عن غيرها من الأنشطة الاجرامية ، فهى جرائم غير تقليدية –وغير ملموسة – ويصعب معها أصباغ الحماية على أنظمة الحاسوب – من برامج وبيانات – من خلال النصوص التقليدية الواردة فى قانون العقوبات . مما حد بالتشريعات المختلفة إلى الإنتباه إلى ضرورة مواجهة الإجرام المعلوماتى La guminalité informatique بنصوص تشريعية جديدة تتلائم مع الطبيعة الخاصة لهذه الجرائم .

وسوف نعرض للجريمة المعلوماتية فى الاتفاقيات الدولية، من خلال الدراسات التالية:

**المبحث الأول: الجريمة المعلوماتية في إتفاقية بودابست 2001 .**

**المبحث الثاني: إتفاقية الجرائم المعلوماتية (المجلس الأوروبي).**

# المبحث الأول

## الجريمة المعلوماتية فى إتفاقية بودابست ٢٠٠١

من منطلق الجوانب المظلمة التى خلفها مذهب ما بعد الحداثة ، حرص المجلس الأوروبى على التصدى للاستخدام غير المشروع للحاسبات وشبكات المعلومات ، وتجلى ذلك فى إتفاقية بودابست الموقعة فى ٢٣ نوفمبر ٢٠٠١ المتعلقة بالإجرام الكونى Convention Sur La Cyber Criminalité, Budapest, 23, X 1. 2001 بمعنى الإجرام المعلوماتى أو الجرائم المعلوماتية ، إيماناً من الدول الأعضاء فى هذا المجلس والدول الأخرى الموقعة على هذه الاتفاقية «...بالتغيرات العميقة التى حدثت بسبب الرقمية La numérisation (*) ، والتقارب La Convergence (**) العولمة المستمرة La mondialisation Perma-nente للشبكات المعلوماتية des réseaux informatiques » (1) .

(*) ويقابل هذا فى الطبعة الإنجليزية : the digitalisation وهذه الكلمة مشتقة من digit وتعنى ماهية الشئ حين يعبر عنه بالنظام الثنائى بدلاً من صور التعبير المعتادة التناظرية an-alog والاتصالات الرقمية هى نقل الإشارات بعد تحويلها للصورة الرقمية بدلاً من نقلها كموجات تناظرية . والحاسب الرقمى digital computer هو ذلك الذى يعمل بالنظام الثنائى حيث تحول البيانات فيه إلى الصورة الرقمية وتتم معالجتها عن طريق عملية التكويد Cod-ing– والحاسب الرقمى يقابل الحاسب التناظرى analog computer الذى ليس له إلا استخدامات محدودة فى بعض المجالات البحثية . والصناعية كحل المعادلات الرياضية (لمزيد من المعرفة راجع د. عبد الحليم شوشة : «الإلكترونيات وتطبيقاتها فى الإتصالات والحاسبات والتحكم » – مرجع سابق – سنة ٢٠٠٢ ، ص١٠٨ وما بعدها، نيكولاس نيجروبرنت : « التكنولوجيا الرقمية ثورة جديدة فى نظم الحاسبات والاتصالات ، ترجمة أ. د. سمير إبراهيم شاهين ، القاهرة ، مركز الأهرام للترجمة والنشر ١٩٩٨ ، على يوسف على : « معجم مصطلحات الحاسب » – مرجع سابق – ص٢١٣ وما بعدها) .

(**) ويعنى التقارب فى مجال التقنيات : تقارب بين تقنيتين مثل التقارب بين الاتصالات والحاسب فى الشبكات المعلوماتية (على يوسف على المرجع السابق ص١٦٥) .

(1) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية – مرجع سابق – ص ٢٩ .

وكما تضمنت المذكرة التفسيرية Rapport explicatif لهذه الإتفاقية : هناك سمة بارزة فى تكنولوجيا المعلومات تتمثل فى الأثر الذى أحدثته ومازالت تحدثه على تطور تكنولوجيا الاتصالات عن بعد .

وتتكون هذه الإتفاقية من ثمانى وأربعين مادة موزعة على أربعة أبواب (١) :

يعالج **الباب الأول chapitre I** : استخدام المصطلحات Terminologie .

ويتناول **الباب الثانى chapitre II** : الإجراءات الواجب إتخاذها على المستوى القومى Mesures à prendre au niveau national – ويضم ثلاثة أقسام:

القسم الأول– القانون العقابى المادى أو الموضوعى Droit pénal matéreil .

القسم الثانى – القانون الإجرائى Droit procédural .

القسم الثالث – الاختصاص القضائى Compétence .

**الباب الثالث chapitre III** :: تم تخصيصه لدراسة التعاون الدولى coopération internationale ... وهو يشتمل على قسمين :

القسم الأول – المبادئ العامة Principes internationale .

القسم الثانى – الأحكام الخاصة Dispositions specifiques .

وأخيراً **الباب الرابع chapitre IV** :: يتعرض للشروط الختامية clauses finales .

وقد تم التمهيد لهذه الأبواب الأربعة بافتتاحية (مقدمة) preambule . ونظراً لأن موضوع دراستنا ينصب على الحماية التشريعية للمعلوماتية فى اطار

---

(١) يراجع بشأن هذه الإتفاقية: د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٣٠ وما بعدها.
د/ عمر محمد بن يونس – الإتفاقية الأوروبية للجريمة الافتراضية – بدون ناشر – طبعة أولى معربة – سنة ٢٠٠٥.

الأمن المعلوماتى ... وذلك بتجريم الأفعال المخالفة التى تتناول المعلوماتية وحصرها فى نطاق الجريمة المعلوماتية . والتى قطع المجتمع الدولى فيها مراحل متميزة، وأبلى بشأنها بلاء حسن من حيث تجريم الأفعال التى تنتهك المعلوماتية، وحصر الجرائم المعلوماتية ، من خلال النص عليها فى الإتفاقيات الدولية التى تتناول نظم المعلوماتية ، سابقًا بذلك التشريعات الوطنية التى – فى معظم الدول – أحالت الموضوع برمته للتشريع الجنائى السارى بها والذى يحوى النصوص العامة والقواعد القانونية التقليدية .

وسوف نتناول بالعرض – الذى يفيد أغراض الدراسة – من هذه الإتفاقية الموضوع الثانى المتعلق بالقانون الأساسى وقانون الاجراءات الجنائية ، ونجتزئ منه الشق الأول الخاص بالقانون الأساسى (قانون العقوبات) والذى يشتمل على تسع جرائم معلوماتية مقسمة على أربع فئات رئيسية :

أ– الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتية.

تناولتها من الاتفاقية المواد الآتية: –

(المادة ٢) – الولوج غير القانونى .

(المادة ٣) – الاعتراض غير القانونى .

(المادة ٤) – الاعتداء على سلامة البيانات .

(المادة ٥) – الاعتداء على سلامة النظام .

(المادة ٦) – إساءة استخدام أجهزة الحاسب .

ب– الجرائم المعلوماتية (الجرائم المتصلة بالحاسب) .

تناولتها من الاتفاقية المادتان: –

(المادة ٧) – التزوير المعلوماتى .

(المادة ٨) – الغش المعلوماتى .

جـ- الجرائم المتصلة بالمحتوى .

(المادة ٩) - الجرائم المتصلة بالمواد الإباحية الطفولية .

د- الجرائم المتصلة بالإعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة .

(المادة ١٠) - الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة .

وتبين المذكرة التفسيرية أن الهدف من القسم الأول من الباب الثانى من الإتفاقية بمواده من ٢ - ١٣ هو تحسين أو إصلاح وسائل منع وقمع الإجرام المعلوماتى Améliorer les moyens de prévenir et de réprimer la criminal-ité informatique وذلك من خلال تحديد معيار بالحد الأدنى المشترك الذى يسمح باعتبار بعض التصرفات من قبيل الجرائم الجنائية .

وتشير المذكرة التفسيرية إلى أن قائمة الجرائم المدرجة فى هذا القسم تمثل الحد الأدنى للتوافق unconsensus minimal الذى لا يستبعد أن يتم استكمال هذه القائمة فى القانون الداخلى ، وأن هذه القائمة تستند إلى درجة كبيرة على المبادئ الواردة فى التوصية la recommandation رقم ٩ لسنة ١٩٨٩ لمجلس أوروبا بخصوص الجرائم المتعلقة بالحاسب وكذلك أعمال المنظمات العالمية الأخرى سواء العامة أم الخاصة ، كما أنها من ناحية أخرى تأخذ فى الاعتبار أيضًا الممارسات غير المشروعة pratiques illicites الأكثر حداثة Plus - ré-centes والمرتبطة بالتوسع فى استخدام شبكات الاتصال عن بعد à l'expansion des réseaux de Telécommunications. [1] .

ويتفرع القسم الأول إلى خمس عناوين Titres رئيسية هى[2] :

العنوان الأول Le Titrel: ويضم جوهر جرائم الحاسب أو الجرائم المعلوماتية

---

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص٥٦ .

(٢) المرجع نفسه - ص٥٧ وما بعدها .

les infractions informatiqucs تلك الجرائم التى تعرف بالجرائم ضد سرية البيانات ، وسلامة البيانات والنظم وإتاحة البيانات والنظم ، وهذه الجرائم تمثل التهديدات الرئيسية وفقًا للمناقشات التى دارت حول أمن الحاسبات والبيانات – والتى تؤثر على نظم المعالجة الآلية وإرسال البيانات .

وتشتمل العناوين من ٢ – ٤ على نوعية أخرى من جرائم الحاسب أو الجرائم المعلوماتية ، وهى التى تلعب دوراً أكبر فى الممارسة العملية ، حيث يتم استخدام أجهزة الحاسب والإتصالات كوسيلة للهجوم على بعض المصالح القانونية certains intérets juridiques والتى كقاعدة عامة، يحميها مسبقًا قانون العقوبات، من هذه الهجمات عن طريق استخدام الوسائل التقليدية à l'aide de moyens classiques .

**العنوان الثانى Le Titre 2** : وقد تم إضافة جرائم هذا العنوان وهى الغش المعلوماتى le fraude informatique والتزوير المعلوماتى la falsification in-formatique من خلال الاقتراحات التالية لتوصية مجلس أوروبا رقم ٩ لسنة ١٩٨٩ .

**العنوان الثالث Le Titre 3** : ويغطى الجرائم المرتبطة بالمحتوى les infractions se rapportant ou contenu ، بمعنى الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية عبر النظم المعلوماتية ، والذى يمثل أحد نماذج تنفيذ الجريمة الأكثر خطورة ، والذى بدأ فى الظهور حديثاً .

**العنوان الرابع Le Titre 4** : يحدد الجرائم المتعلقة بالاعتداء على الملكية الفكرية والحقوق المرتبطة بها Leb infractions liées aux atteintes à la propriété intellectuelle et aux drouts connexes. وقد نصت الاتفاقية على هذه النوعية من الجرائم، وذلك لأن الانتهاكات الواقعة على الملكية الفكرية هى أحد أشكال الإجرام المعلوماتى الأكثر شيوعاً، والذى باز ديار نسبته يزداد قلق أو انشغال العالم بأسره.

العنوان الخامس Le Titre 5، يشتمل على أحكام إضافية بخصوص الشروع La Tentative والاشتراك Complicité ، وأيضاً الجزاءات والإجراءات أو التدابير، وذلك طبقاً للمعايير الدولية الحديثة، بالنسبة لمسئولية الأشخاص المعنوية.

وإذا كانت نصوص قانون العقوبات تنطبق على الجرائم المرتكبة عن طريق تكنولوجيا المعلومات، فإن المذكرة التفسيرية حرصت على إيضاح أن الاتفاقية تستخدم مصطلحات تكنولوجية محايدة Neutre بطريقة يمكن معها تطبيق جرائم قانون العقوبات على كلا من التكولوجيات الآتية والمستقبلية.

ومن النقاط الهامة التى ركزت عليها المذكرة التفسيرية أيضاً ضرورة أن يكون ارتكاب الجرائم المحصاة فى هذه الاتفاقية «دون حق» ويتجلى ذلك فى قولها: (يشترط فى تجريم الأفعال المذكورة فى هذه الاتفاقية أن يكون القيام بالفعل دون حق Sans Droit).

كذلك تقرر المذكرة التفسيرية أن كل الجرائم المدرجة فى هذه الاتفاقية يجب أن تكون مرتكبة بطريقة عمدية Facon Intentionnelle من أجل تقرير المسئولية الجنائية، وفى بعض الحالات يتطلب الأمر عنصراً عمدياً خاصاً، أو بتعبير آخر قصد خاص لاستكمال عناصر الجريمة، مع ترك المعنى الدقيق لكلمة عمد أو قصد للقوانين الداخلية.

- وسوف نتناول فيما يلى الجرائم الواردة فى العناوين من الأول إلى الرابع وهى تشمل المواد من ٢ إلى ١٠:

- **العنوان الأول:** الجرائم ضد سرية وسلامة وإتاحة البيانات والنظم المعلوماتى Infractions contre la confidentialité, l'intégrit et la disponibilité des données et systémes informatique. تشير المذكرة التفسيرية إلى أن الغرض من الجرائم الجنائية التى تناولها هذا العنوان هو حماية سرية وسلامة وإتاحة أو تهيئة البيانات ونظم الحاسب للعمل أو التشغيل، وبالتالى يخرج من

نطاق التجريم الأنشطة المشروعة والعادية والمرتبطة بتصميم الشبكات، وكذلك الممارسات الاستثمارية أو التجارية المشروعة والعادية.

وقد تناولت المواد (٢-٦) جرائم هذا العنوان على النحو التالى[١]: -

**المادة ٢: الولوج غير القانوني Accés Illégal[٢]:**

**النص:** يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الداخلى، للولوج العمدى لكل أو لجزء من جهاز الحاسب بدون حق. كما يمكن له أن يشترط أن ترتكب الجريمة من خلال انتهاك إجراءات الأمن، بنية الحصول على بيانات الحاسب أو أية نية إجرامية أخرى، أو أن ترتكب الجريمة فى حاسب آلى يكون متصلاً عن بعد بحاسب آخر.

**التعليق:** تقرر المذكرة التفسيرية أن الولوج غير القانونى يعد الجريمة الرئيسية التى تنطوى على تهدد وتعد على أمن بمعنى السرية والسلامة، والإتاحة للنظم والبيانات المعلوماتية، إذ إن هناك ضرورة لتوفير حماية ملائمة لمصالح المنظمات، وبالأخص لرجال الإدارة حتى يكون بمقدورهم أن يديروا، ويستثمروا ويتحكموا فى نظمهم بدون تشويش أو عقبة من أى نوع.

وعلى ذلك، فإن مجرد التدخل غير المصرح به بمعنى القرصنة[٣] Le Piratage أو السطو Le Craquage أو الدخول غير المشروع فى النظام المعلوماتى، كل أولئك يجب أن يعتبر غير قانونى فى حد ذاته كمبدأ عام.

(١) د/ هلالى عبد الله أحمد – المرجع السابق – ص ٦٨ وما بعدها.

(٢) ويقابل ذلك فى المصطلح الإنجليزى. - Illegal access

(٣) أشارت المذكرة التفسيرية إلى أن العديد من التشريعات الداخلية سبق أن تضمنت نصوصاً تتعلق بالجرائم المرتبطة بالقرصنة، لكن نطاقها والعناصر المكونة لها متنوعة أو متباينة للغاية. والخلاصة أنه يمكن لأطراف الاتفاقية أن يتبنوا المدخل العام وأن يقوموا بتجريم القرصنة بلا قيد أو شرط وفقاً للمادة الأولى من المادة الثانية.

ويضم الولوج غير القانونى، أو الولوج غير المصرح به، الأختراق La Pénétration الذى يحدث للنظام بأكمله، أو لجزء منه أيا كان، إذ يستوى أن يكون جزءاً مادياً، أو برامج جزئية، أو بيانات مخزنه فى نظام التنصيب(*) Données stockéedu syst.éme installé أو فهارس أو بيانات تتعلق بالمرور والمحتوى.

وبالإضافة إلى أن الولوج غير القانونى يضم الاختراق الذى يحدث للنظام بأكمله أو لجزء منه، فإنه يضم أيضاً الاختراق الذى يحدث لنظام معلوماتى متصل بشبكات أتصال عامة، أو لنظام معلوماتى متصل بنفس الشبكة، أى شبكة محلية أو إنترنت Unintranet أو شبكة خاصة لشركة (منظمة) Réseau Privé D'entreprise.

**المادة ٣: الاعتراض غير القانوني Interception Illegal(١):**

**النص:** يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات أخرى يرى إنها ضرورية من أجل اعتبارها جريمة جنائية، وفقاً لقانونه الداخلى، واقعة الأعتراض العمدى وبدون حق، من خلال وسائل فنية للإرسال غير العلنى، لبيانات الحاسب فى مكان الوصول، فى المنشأ، أو فى داخل النظام المعلوماتى. بما فى ذلك الانبعاثات الكهرومغناطيسية من جهاز حاسب يحمل هذه البيانات.

**التعليق:** تقرر المذكرة التفسيرية أن الهدف من نص المادة الثالثة هو حماية الحق فى أحترام نقل البيانات(٢)، وأن هذه الجريمة تمثل انتهاكاً للحق فى أحترام

---

(*) يقصد بنظام التنصيب عموماً دمج برنامج معين فى نظام الحاسب وتجهيزه للعمل، ويستخدم لذلك برنامج يسمى Installation Program. (م/ على يوسف على – مرجع سابق – ص ٣٦٦).

(١) ويقابل ذلك فى النص الإنجليزى Illegal interception. (الاعتراض غير المشروع).

(2) Le droit au respect des données transmises.

الاتصالات[1] مـثل التـصنت[2] والتسجيل التقليدى للمحادثات التليفونية بين الأشخاص[3]، كما أن الحق فى احترام المراسلات[4] مكفول عن طريق المادة الثامنة من الاتفاقية الأوروبية لحقوق الإنسان La conventicn européenne des droits de l'homme والجريمة المنصوص عليها فى المادة الثالثة تطبق هذا المبدأ على كل أشكال النقل الإلكترونى للبيانات à toutes les formes de tranfert électronique des données، سواء تم هذا النقل عن طريق التليفون Téléphone أو الفـاكس Télécopieur أو البـريد الإلكترونى Courier électronique أو نقل الملفات Fichier.

كما أشارت المذكرة التفسيرية إلى المصدر الذى أخذت عنه المادة الثالثة بقولها: إن نص هذه المادة قد اشتق بشكل أساس من جريمة الاعتراض غير المصرح به L'infraction d'interception non autorisés[5] المنصوص عليها فى التوصية رقم (٨٩) ٩، وفى الاتفاقية الحالية تم توضيح أن مفهوم الاتصالات Communications[6] يمتد ليشمل «وسائل نقل بيانات الحاسب Les transmission... de données informatiques»[7]، وكذلك انبعاثات الإشعاع الكهرومغناطيسى Les émissions électromagnétiques[8]، فى ظل المواقف الموضحة فيما بعد.

---

(1) Le droit au respect des communications.

(2) L'ecoute.

(3) L'enregis trement classiques des conversation téléphoniques entre des personnes

(4) Le droit au respect de la correspondance.

(٥) ويقابل ذلك فى المصطلح الإنجليزى. The offence of unauthorised interception

(٦) ويقابل ذلك فى المصطلح الإنجليزى. The communications

(٧) ويقابل ذلك فى المصطلح الإنجليزى. Transmissions of computer data

(٨) ويقابل ذلك فى المصطلح الإنجليزى. Electromagnetic radiation

ويتم الاعتراض L,interception باستخدام وسائل فنية Des moyens techniques تتعلق بالتنصت L'écoute أو التحكم Le contrôle أو مراقبة محتوى الاتصالات La Surveillance du contenu des communications[1]، والحصول على المحتوى بطريقة مباشرة من خلال طريقة الولوج إلى داخل النظام المعلوماتي واستخدامه، أو بشكل غير مباشر عن طريق استخدام أجهزة التنصت L'emploi de dispositifs d'écoute[2] كذلك يمكن أن تشتمل وسائل الاعتراض على تسجيل البيانات Un enregistre ment des données، ليس هذا فحسب، بل إن نطاق الوسائل الفنية يجب أن يمتد ليشمل الأجهزة الفنية المتصلة بخطوط النقل أو الاتصال Des dispositifs techniques connectés aux lignes de transmission[3] مثل أجهزة تجميع وتسجيل الاتصالات اللاسلكية des dispositoifs de collecte et d'enregistrement de communications sans fil كما يمكن أن تشمل أيضاً الكيانات المنطقية Logiciels، وكلمات المرور Mots d'accés، والشفرات Codes.

وجدير بالذكر أن اشتراط استخدام وسائل فنية – كتلك التى سلف ذكرها – يعد شرطاً مقيداً لتجنب عقبة (مشكلة) العقاب المبالغ فيه à éviter L'écueil de la surpénalisation[4].

وجريمة الاعتراض غير القانونى تنطبق على وسائل النقل غير العلنية

---

(١) ويقابل ذلك فى المصطلح الإنجليزى.
Surveillance of the content of communications

(٢) ويقابل ذلك فى المصطلح الإنجليزى.
The use of electronic eavesdropping or tapping devices

(٣) ويقابل ذلك فى المصطلح الإنجليزى.
Devices to collect and record wireless communications

(٤) ويقابل ذلك فى الطبعة الإنجليزية. To avoid over - eriminalisation

لبيانات الحاسب S'applique aux transmissions non publique de données[1]
ويلاحظ أن مصطلح «غير العلنية Non publiques»، صفة تتبع طبيعة وسيلة النقل أو الاتصال Qualifie la nature du moyen detransmission ou communication[2] وليس طبيعة البيانات المرسلة. فالبيانات المرسلة يمكن أن تكون مهيأة Disponibles لكل الناس Pour tout le monde، لكن الأطراف يرغبون فى الاتصال بطريقة سرية De façon confidentielle[3]، كما يمكن أيضا الاحتفاظ بالبيانات بصورة سرية لأغراض تجارية، حتى يتم دفع مقابل الخدمة، كما فى حالة التليفزيون بالاشتراك La télévisons payante، وعلى ذلك، فإن مصطلح «غير العلنية Non publiques»، لا يستبعد الاتصالات فى حد ذاتها عبر الشبكات العامة. فاتصالات العاملين Les communications des salariés[4] سواء لأغراض العمل أم لا، والتى تشمل «وسائل النقل غير العلنية لبيانات الحاسب» هى أيضا محمية Protégées ضد الاعتراض L'interception بمقتضى المادة الثالثة[5].

والاتصال على شكل نقل بيانات الحاسب، يمكن أن يحدث داخل نفس جهاز الحاسب à L'intérieur d'un méme systéme informatique، كما فى حالة الدورة بين وحدة المعالجة المركزية والشاشة والطابعة. كما يمكن أن يتم هذا الاتصال

---

(١) ويقابل ذلك فى الطبعة الإنجليزية.
Applies to non - public transmissions of computer data
(٢) ويقابل ذلك فى المصطلح الإنجليزى.
Qualifies the nature of the transmission or communication process
(٣) ويقابل ذلك فى المصطلح الإنجليزى. To communicate confidentially
(٤) ويقابل ذلك فى المصطلح الإنجليزى. Communications of employees
(٥) ومن التطبيقات القضائية راجع:
L'arrét rendu par la CEDH dans l'affaire Halford C. Royaume - Uni, 25 juin 1997, 20605/92.
مشار إليه لدى دكتور/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٨١.

بين جهازين لنفس المالك، أو بين جهازين متصلين ببعضهما البعض، أو بين جهاز وشخص، كما هو الحال فى حالة تعامل الشخص مع لوحة المفاتيح Le biais du clavier، ومع ذلك... يمكن للأطراف أن يشترطوا شرطاً أضافياً Condition supplémentaire كأن يكون الاتصال بين الجهازين عن بعد à distance[١].

**المادة ٤: الأعتداء علي سلامة البيانات (التداخل أو التشويش علي البيانات) Atteinte à lintégrité des données[٢]:**

**النص:** ١- يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم - تبعاً لقانونه المحلى - إذا حدث ذلك عمداً، ودون حق، أى اضرار، أو محو، أو تعطيل، أو إتلاف، أو طمس لبيانات الحاسب.

٢- يمكن لأى طرف أن يحتفظ بحق اشتراط أن يكون السلوك المنصوص عليه فى الفقرة الأولى يؤدى إلى أضرار جسمية.

**التعليق:** تشير المذكرة التفسيرية إلى أن الهدف من تقرير هذا النص هو أن تكون بيانات وبرامج الحاسب مكفولة بحماية مماثلة Une protection analogue لتلك التى تتمتع بها الأشياء المادية ضد الأضرار التى تحدث عمداً، والمصالح القانونية المحمية هى سلامة وحسن تشغيل، أو حسن أستخدام البيانات أو برامج الحاسب المسجلة.

---

(١) تجدر الاشارة إلى أن عبارة (جهاز الحاسب أو النظام المعلوماتى) يمكن أن تغطى أيضاً الاتصالات اللاسلكية، والتى على الرغم من أنها (غير علنية) إذ إنها تحدث على نحو مفتوح.. يمكن الوصول إليها. ولذلك من السهل اعتراضها وبالأخص بواسطة هواة اللاسكى Des radio amateurs.

(٢) ويقابل ذلك فى النص الإنجليزى. Data interference

وقد ورد فى الفقرة الأولى من المادة الرابعة مصطلح الأضرار L'endommagement ومصطلح التعطيل Détérioration وهى من الأعمال المتراكبة التى تتصل على وجه الخصوص بالإتلاف السلبى L'altération négative لسلامة أو محتوى معلومات البيانات والبرامج، كما ورد فى هذه الفقرة أيضاً مصطلح محو البيانات L'effacement des données وهذا المصطلح يعادل تدمير الأشياء المادية، فهو يهدمها Les détruit ويجعلها فى حالة لا يمكن التعرف عليها.

كذلك ورد فى الفقرة الأولى من المادة الرابعة مصطلح طمس البيانات المعلوماتية La suppression des données informatiques، وهذا المصطلح يمتد ليشمل كل تصرف من شأنه أن يجعل هذه البيانات غير كائنة No sont pas أو غير متاحة accessibles للشخص الذى له حق الولوج إلى داخل الحاسب ،أو الاعتماد على تلك البيانات التى كانت مخزنة.

وأخيراً ورد فى ذات الفقرة مصطلح الإتلاف Le terme altération، وهو يعنى تغيير البيانات الموجودة، وكذلك إدخال شفرات عدوانية، مثال ذلك فيروسات Desvirus(*) أو أحصنة

---

(*) يقابل ذلك فى المصطلح الإنجليزى Viruses.

● تعنى كلمة فيروس فى اللغة تلك الكائنات الدقيقة التى لا ترى بالمجهر العادى وتنفذ من الراشحات البكتيرية وتحدث بعض الأمراض (المعجم الوجيز – مجمع اللغة العربية – القاهرة ١٩٩٠ ص ٤٨٦) والواقع أن هناك وجهاً للشبه بين الفيروس البيولوجى الذى يصيب الإنسان والفيروس الذى يصيب الحاسب الآلى، فإذا كان الفيروس بالمعنى البيولوجى ينقل المرض من شخص مريض إلى آخر سليم حيث يتكاثر داخل جسده، محدثاً تغييراً فى الخصائص العضوية لخلايا الجسم، فإن فيروس الحاسب الآلى يقوم بنفس الغرض، حيث يتكاثر وينتشر داخل النظام المعلوماتى حتى يتسبب فى تغيير وظائفه أو تدميره كلية. (د/ هلالى عبد اللاه – حجية المخرجات الكمبيوترية فى المواد الجنائية) – مرجع سابق – فهرس ص ٧.

د/ ماجد عمار – المسئولية القانونية الناشئة عن أستخدام فيروس برامج الكمبيوتر ووسائل حمايتها – دار النهضة العربية – سنة ١٩٨٩.

طـــروادة Des - chevaux de Troie(*) والتى من شـأنها تغيير البيـانات التى تنــتج عن هــذا التصرف(**).

والتصرفـات السابقة لا يتم المعاقبـة عليـها إلا اذا أرتكبت بدون حق Sans drait. عكس الأنشطة العادية المتضمنة فى تصميم الشبكات، أو تطبيقات شائعة للتشغيل Les pratiques ordinaires d'exploitation أو لممارسات تجارية.

مـثـال ذلك.. تلك التى تطابق مـحـاولات اخـتـيـار أو حـمـاية أمن نظام معلوماتى، والمصرح بها من قبل المالك أو مشغل النظام أو عند اعادة تنظيم نظام تشغيل حاسب à la reconfiguration du systàme d'exploitation d'un[(١)] ordinateur والذى يحدث عندما يقتنى مشغل النظام كياناً منطقياً جديداً Un nouveau logiciel[(٢)].

كما فى حالة تشغيل كيانات منطقيـة للولوج عبـر الإنترنت مما يثبط

---

(*) يقابل ذلك فى المصطلح الإنجليزى Trojan horses.

- ويعتبر فيروس حصان طروادة من أشهر أنواع الفيروسات شيوعاً، وهو عبارة عن برنامج فيروس لديه القدرة على الاختفاء فى البرنامج الأصلى، وعندما يتم تشغيل البرنامج الأصلى ينشط الفيروس وينتشر ليبدأ نشاطه التدميرى الذى قد يؤدى إلى تعديل فى البرنامج الأصلى أو تزوير المعلومات أو محو بعضها، بل قد يصل إلى تدمير النظام المعلوماتى بأسره، ونظراً للمقدرة الفائقة لهذا الفيروس على الاختباء والاختفاء عن أعين المستخدم والتمويه عليه فقد شبه بحصان طروادة الذى استخدمه الإغريق حوالى عام ١٢٠٠ ق.م (لمزيد من التفصيل يراجع: د/ رأفت منير – فيروس الحاسبات وطرق الوقاية – مجلة المهندسين – القاهرة – سنة ١٩٩٠، أ/ حسين حسن بركات – الفيروس جرثومة الكمبيوتر – الدمام – المملكة العربية السعودية – مؤسسة جمال الجاسم للإلكترونيات – ١٩٩٠م، رونالد ميكلين – دليل الوقاية من فيروس الحاسب – ترجمة مركز التعريب والبرمجة – بيروت (لبنان) – الدار العربية للعلوم – سنة ١٩٩٢.

(**) أى ادخال الفيروسات.

(١) ويقابل ذلك فى الطبعة الإنجليزية
The reconfiguration of a Computer's operating Systém

(٢) ويقابل ذلك فى المصطلح الإنجليزى New Software

Désactivent البرامج المماثلة التى أدخلت فيما سبق. كل تلك الأنشطة تعتبر شرعية Légitimes، وبالتالى لا يتم العقاب عليها بواسطة المادة الحالية.

وكقاعدة عامة، فإن تغيير بيانات المرور ddes données de Trafic بهدف تسهيل الاتصالات مجهولة الهوية Les communications an anonymes[1]، مثل أنشطة نظم إعادة إرسال المراسلات مجهولة الهوية des systémes de réexpédition anonyme[2] أو تغيير البيانات بهدف ضمان حماية الاتصالات، مثال ذلك التشفير Chiffrement، كل أولئك يجب أن يعتبر كضمان لحماية مشروعة للحاية الخاصة، وأن الوصول إلى ذلك قد تم بوسيلة شرعية de façon Légitime ومع ذلك، فإن الأطراف يمكن لهم تجريم بعض التصرفات التعسفية Incriminer Certains actes abusifs[3] التى تتعلق بالاتصالات مجهولة الهوية. كما فى حالة تزوير البيانات La falsification des données[4] بغرض إخفاء Dissimuler هوية فاعل الجريمة L'identité de l'auteur d'une infraction[5].

وعلاوة على ذلك فإن الفاعل Le délinquant يجب أن يرتكب الجريمة عمداً Intentionne-LLement.

وجدير بالذكر أن الفقرة الثانية من المادة الرابعة تجيز للأطراف عمل تحفظ à faire une réserve بالنسبة للجريمة، بحيث يمكن أن يشترطوا أن يؤدى السلوك إلى ضرر جسيم Le comportement droit entrainer un préjudice grave وتفسير ما يعد ضرراً جسيماً يترك للتشريع الداخلى[6].

---

(١) ويقابل ذلك فى المصطلح الإنجليزى Anonymous Communications

(٢) ويقابل ذلك فى المصطلح الإنجليزى Anonymous Remailes Systéms

(٣) ويقابل ذلك فى الطبعة الإنجليزية To criminalise certain abuses

(٤) ويقابل ذلك فى الطبعة الإنجليزية The packet header information is altered

(٥) ويقابل ذلك فى المصطلح الإنجليزى The identity of the perpetrator in committing a crime

(٦) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية – مرجع سابق – ص ص ٨٩، ٩٠.

• وقفه تحليلية عن فيروس الحاسب الآلي:

من أهم صور الاستخدام غير المشروع للحاسب، تلك التى تتخذ صورة فيروس يهدد بتدمير الثورة المعلوماتية، والفيروس عبارة عن برنامج يصممه المجرم المعلوماتى بطريقة تعطيه القدرة على ربط نفسه ذاتياً ببرامج أخرى. ثم يتوالد ويتكاثر تلقائياً وينتشر داخل البرامج المختلفة أو بين مواقع معينة من ذاكرة الحاسب حتى يحقق الأهداف المتوخاه منه. وهو تيميز بعدة سمات(١):

أولها – قدرته على إخفاء نفسه عن المستخدم والتمويه عليه.

ثانيها – قدرته على الانتشار من حاسب إلى آخر داخل شبكة الاتصالات.

ثالثها – قدرته على التسلل إلى داخل النظام واختراق موانع الأمن.

رابعها – قدرته على التدمير، بمعنى مسح البيانات المخزونة على وسائط التخزين(٢).

وتتعدد أنواع فيروسات الحاسب الآلى، وإن كان أكثرها شيوعاً فيروس حصان طراودة، فإنه يوجد كذلك فيروس القنبلة المعلوماتية الموقوتة(*)، وفيروس الدودة المعلوماتية(**).

---

(١) د/ هلالى عبد اللاه أحمد – حجية المخرجات الكمبيوترية فى المواد الجنائية – مرجع سابق – ص ص ٧، ٨.

(٢) ويطلق المتخصصون فى مجال الحاسب على هذه العملية مصطلح Zeroing أى مسح البيانات وتحويلها إلى حرف Zero. للمزيد يراجع:

- PARKER (Doon): "Computer crime" Publishedin: Computer security Refrence book, U.S.A. 1992, p. 438.

(*) القنبلة الموقوته Time bomb هى نوع من الفيروس يظل كامناً، وبالأخص فى ذاكرة الحاسب، ولا ينشط ويبدأ فى التدمير إلا عند حدوث واقعه معينة كأن تكون كلمة محددة يكتبها المستخدم أو تاريخ يوم معين يتم تحديده فى ساعة الحاسب.

(**) فيروس الدودة Warm هو عبارة عن برنامج فيروس يتميز بقدرته الفائقة على تعطيل وإيقاف نظام الحاسب الآلى بأكمله، وأول من أستخدم هذا الفيروس شاب أمريكى يدعى روبرت تابان موريس Robert T. Morris سنة ١٩٨٨ وهو خبير فى أمن الحاسبات كان يجرى بعض

=/=

كما تتعدد الأغراض المتوجاة من زراعة فيروس الحاسب الآلى، وأهمها(١):

- اختراق النظام المعلوماتى لأحد البنوك بغرض تحويل مبالغ مالية من حسابات العملاء إلى الحساب الخاص للمجرم المعلوماتى(*).
- اختراق النظام المعلومتى للغير لنقل المعلومات المعالجة إلكترونياً، أو لنقل برنامج من برامجه كلياً أو جزئياً إلى النظام الخاص بالمجرم المعلوماتى(**).

---

-- التجارب على أمن الحاسبات بمعمل الذكاء الاصطناعى بمعهد ماساشوسيتس للتكنولوجيا، والتابع لجامعة كورنل Cornel التى كان موريس مسجلاً بها درجة الدكتوراه، فاكتشف ثغرة Hole فى شبكة أربانيت A RPANET وهى من أكبر وأخطر شبكات الحاسب فى U.S.A حيث إنها تربط بين القوات المسلحة والجامعات ومعاهد البحث العلمى. فقام بإطلاق فيروس الدودة فى هذه الثغرة التى اكتشفها ليختبر مدى قدرة الشبكة على كشف هذه الدودة وعزلها عن النظم المعلوماتية المشاركة فيها. فإذا بهذه الدودة تفلت من سيطرة موريس وتنتشر بسرعة مذهلة فاضطر إلى إبلاغ السلطات المختصة بعد أن أدت تجربته إلى توقف حوالى ٦٢٠٠ جهاز حاسب عن العمل وخسائر تقدر بمائة مليون دولار. وقد تمت محاكمة موريس جنائياً طبقاً للقانون الفيدرالى الصادر سنة ١٩٨٦ بشأن الغش وإساءة استخدام الحاسب. راجع:

- MICHAEL (Alexander): :Morris sentence spurs debate" computer world Vol. 24, No, 20, May 14, 1990 - Morris contemplates supreme court option "Computer world" Vol. 25, No. 11, March 18, 1991, Vol. 25, No. 11, March 18, 1991.

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٩ وما بعدها.

(*) ومن التطبيقت القضائية لهذا الغرض قضية تخلص وقائعها فى.. قيام أحد خبراء البرمجة – أمريكى الجنسية – ويدعى ستانلى ريفكن Stanly rifkin، بالتقاط الشفرة التى يستخدمها بنك Security Pacific فى مدينة لوس أنجلوس بولاية كاليفورنيا فى إجراء تحويلات العلماء من خلال التسلل إلى غرفة الأسلاك البرقية المركزية لهذا البنك. وعن طريق الهاتف تمكن من الاتصال بشبكة معلومات البنك مستخدماً الشفرة التى حصل عليها وقام بزراعة برنامج فيروس فى هذه الشبكة مهمته تحويل مبالغ مالية من حسابات البنك إلى حسابه الخاص فى نيويروك. وبالفعل استطاع ريفكن تحويل مبالغ وصل مجموعها ١٠,٥ مليون دولار. يراجع فى ذلك.

- Computer Bank, Bankers Review security procedures after virus Attack. Bol. 6 No. 1, January, 1988, p. 8.

(**) من أبرز التطبيقات العملية لهذا الغرض.. ما حدث فى ولاية كاليفورنيا من قيام المدعو/ وارد WARD باختراق النظام المعلوماتى لمكتب خدمة مشاركة فى وقت الحاسب، حيث قام بزراعة برنامج فيروس بهدف نقل المعلومات الخاصة بهذا المكتب إلى نظامه المعلوماتى راجع:

-/-

- اختراق النظام المعلوماتى للغير بغرض التجسس على المؤسسات الهامة فى الدولة، أو التجسس على الأسرار الشخصية للأفراد أو التلاعب فى بياناتهم ذات الصفة الشخصية بالحذف أو الإضافة أو التعديل(*).
- اختراق النظام المعلوماتى للاستفادة من إمكانات الحاسب الآلى ذاته، وهو ما يطلق عليه سرقة وقت الحاسب(**).

---

- Bigelow (R.): "The legal dimension of computer crime" EDP - Aditor-Jornal, Vol. 2. 1995, p. 59.
- ومن تطبيقات هذه الحالة أيضاً ما عرض على القضاء الأمريكى من قيام أحد الموظفين بشركة University-Computing Company بزراعة برنامج فيروس فى النظام المعلوماتى لشركة In formation system Design أستطاع بمقتضاه أن ينقل نسخة كاملة من أحد برامج هذه الشركة. فعاقبه القضاء بعقوبة السرقة.

(*) من التطبيقات القضائية لهذه الحالة ما قام به كل من مارك لوتور وربرت جيلجن وكيفين بولسن فى يناير ١٩٩٠ بالتسلل عن طريق برنامج فيروسى لنظام حاسب متعلق بالقوات المسلحة الأمريكية والحصول على معلومات سرية مخزونة بداخل هذا النظام. بالأضافة لقيام كيفين بولسن عن طريق برنامج فيروسى بالاستيلاء على معلومات سريه للغاية من حاسب شركة بل Bell للتليفونات كانت تتعلق بتحقيقات سرية كان مكتب التحقيقات الفيدرالية الأمريكى يجريها، حول ودائع الرئيس الفلبينى فريدناند ماركوس فى .U.S.A راجع:

- Mathew (J. Gray): "An ounce of prevention fights computer viruses from electronic vandolism is vital "Tutoriel, Lan time, Vol. 7, No. 14, Nov. 1990. p. 69.

(**) من التطبيقات القضائية لهذا الغرض قيام طالب كندى يدعى Michael Mac بالحصول على وقت وخدمات حاسب جامعة البرتا Alberta بدون وجه حق. بيد أن المحكمة الكندية العليا برأت ساحته على أساس أن جريمة السرقة لا تتوافر فى حقه. ولذا تم تعديل قانون العقوبات الكندى سنة ١٩٨٥ ونص فى الفقرة الثانية من المادة ٣١٠ على معاقبة كل من قام بغش وبدون وجه حق بالحصول مباشرة أو بطريق غير مباشر على أى خدمة من خدمات الحاسب راجع:

- DENNING (Peter): "Computer under Attack" Previous Refrence, p. 115.

- اختراق النظام المعلوماتى للغير لتدمير ثروته المعلوماتية كلها أو جزء منها(*).

**المادة ٥: الاعتداء علي سلامة النظام Atteinte à L'intégritédu Systéme(١):**

النص: يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لتجريم - تبعاً لقانونه المحلى - الإعاقة الخطيرة إذا تم ذلك عمداً، ودون حق لوظيفة نظام الحاسب، عن طريق إدخال أو نقل أو إضرار أو محو أو تعطيل أو إتلاف أو طمس البيانات المعلوماتية.

---

(*) من التطبيقات القضائية لهذه الحالة واقعة مفادها قيام إحدى شركات السمسرة والتأمين على الحياة فى فورت ورث Fort warth بولاية تكساس Texas الأمريكية عام ١٩٨٥ بفصل أحد العاملين بها وهو ضابط أمن لنظم الحاسبات يدعى رونالد جين بيرلسون Donald Gen Burleson. فمن باب الانتقام قام هذا الموظف المفصول باختراق النظام المعلوماتى للشركة المذكورة، مستغلاً فى ذلك ما يسمى بالباب الخلفى للنظام Back Door وزرع قنبلة موقوته استطاعت أن تمحو أكثر من ١٦٨,٠٠٠ سجل من سجلات عمولة المبيعات وأن تغلق النظام، وقد تم ضبط هذا المخرب وحكم عليه القضاء الأمريكى بسبع سنوات تحت المراقبة ودفع تعويض قدرة ١١,٨٠٠ دولار. راجع:

- EDWRD (Jogce): "Computer Decision, Time bomb inside the texas virus trial: vol. 20, Issue No, 12, p. 38.
- COOPER (James Arin): "Computer and communications security" Mc Graw - Hill Book compent, 1990. p. 224.

مشار إليه لدى: د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١١.

(١) ويقابل ذلك فى الطبعة الإنجليزية System interference

التعليق: توضح المذكرة التفسيرية[1] أن التوصية رقم (٨٩) قد أشارت إلى هذا العنوان تحت مسمى... تخريب نظام الحاسب Sabotage informatique[2]، ويهدف هذا النظام إلى تجريم الإعاقة العمدية للأستخدام الشرعى للنظم المعلوماتية، بما فى ذلك نظم الاتصالات، باستخدام أو التأثير على بيانات الحاسب.

والمصالح القانونية المحمية هى مصلحة مشغلى ومستخدمى نظام الحاسب، أو نظام الأتصالات فى عمل هذه الأجهزة بدقة، وتتم صياغة النص بطريقة محايدة من أجل حماية كل أنواع الوظائف من خلاله.

ومصطلح، الإعاقة Entrave، يرتبط بالأفعال التى تحمل اعتداءً على حسن تشغيل نظام الحاسب، وهذه الإعاقة يجب أن تكون ناجمة عن الإدخال L'introduction، أو النقل Du Transfert، أو الإضرار L'endommagemént، أو المحو L'effacement، أو الإتلاف L'altération أو طمس La suppression البيانات المعلوماتية[3].

علاوة على ذلك، فإن الإعاقة يجب أن تكون جسيمة حتى يترتب عليها جزاءً جنائياً ويجب على كل طرف أن يحدد الشروط التى يجب توافرها كى تعتبر الإعاقة جسيمة، على سبيل المثال، يمكن لأى طرف أن يشترط حدوث قدر ذى حد أدنى من الضرر Un dommage d'une importance minimale. لكى تعتبر الإعاقة جسيمية.

وعموماً فإن واضعى الاتفاقية يعتبرون الإعاقة جسيمة، عندما تكون البيانات المرسلة من الحجم Le Volume أو التواتر La fréquence ما يحمل

---

(١) راجع باللغة الفرنسية المذكرة التفسيرية لاتفاقية بودابست ٨ نوفمبر ٢٠٠١، وراجع باللغة الانجليزية مسودة المذكرة التفسيرية لاتفاقية بودابست ستراسبورج ١٤ فبراير سنة ٢٠٠١.

(٢) يقابل ذلك فى المصطلح الإنجليزى Computer Sabotage

(٣) د/ هلالى عبداللاه أحمد – الجوانب الموضوعية والإجرائية لجرائم المعلوماتية – مرجع سابق – ص ٩٢ وما بعدها.

ضرراً جسيماً Un préjudice important لقدرة المالك أو المشغل بالنسبة لاستخدام الجهاز أو الاتصال بالأجهزة الأخرى. مثال ذلك البرامج التى تحمل اعتداءً على النظم، والتى تأخذ شكل «الامتناع عن الخدمة Un déni de service[1]، أو الشفرات العدوانية Des codes malveillants[2]، كالفيروسات التى تمنع Interdisent أو تبطئ Ralentissent بشكل ملموس عمل الجهاز، أو البرامج التى ترسل مقدراً هائلا Un énorme volume من البريد الإليكترونى إلى مرسل إليه Un destinataire من أجل شل Paralyser وظائف اتصال نظام الحاسب.

وفى كل الحالات، يجب أن تكون الإعاقة L'entrave «دون حق Sans droit». فالأنشطة الشائعة المتضمنة فى تصميم الشبكات، أو الممارسات الخاصة بالتشغيل أو التجارة، كل أولئك يكون بحق "Avec droit". إذ إن الأمر يتعلق على وجه الخصوص، بأنشطة اختبار أمن نظام الحاسب أو حماية النظام والمصرح بها من المالك أو القائم بتشغيله، أو عند إعادة تنظيم نظام تشغيل حاسب، والذى يحدث عندما يقتنى مشغل النظام كياناً منطقياً جديداً Un Nouveau Logiciel كما فى حالة تشغيل كيانات منطقية للولوج عبر الإنترنت، مما يثبط البرامج المماثلة التى أدخلت من قبل كل تلك الأنشطة تعتبر شرعية، وبالتالى لا يتم العقاب عليها، بواسطة هذه المادة حتى ولو ترجمت على أنها إعاقة جسيمة Si elles se traduisent par une entrave grave[3].

إن إرسال رسائل إليكترونية L'envoi de messages électroniques لأغراض تجارية أو لأغراض أخرى، لمرسل إليه غير مطالب باستقبالها، يمكن أن تسبب له مضايقات Des désagrément[4] وبالأخص تلك الرسائل التى يتم

---

(١) ويقابل ذلك فى الطبعة الإنجليزية Denial of Service

(٢) ويقابل ذلك فى المصطلح الإنجليزى Malicious codes

(٣) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٩٤.

(٤) ويقابل ذلك فى المصطلح الإنجليزى Nuisance

إرسالها غالباً وبكميات ضخمة. كما هو الحال فى تجارة البريد Publipostage.
وفى رأى واضعى الاتفاقية، فإن مثل هذا السلوك لا يجب أن يكون مجرماً إلا فى حالة الإعاقة العمدية والجسمية بالنسبة للاتصال.

ومع ذلك للأطراف اختيار مفهوم مختلف للإعاقة فى قانونهم الداخلى. إذ يمكن على سبيل المثال اعتبار بعض أعمال التدخل Certains actes d'ingérence(١) من قبيل الجرائم الإدارية Des infractions administratives أو أنها تستحق الجزاء بطريقة أخرى.

وجدير بالذكر أن النص يترك للأطراف مهمة تحديد فى أى الأحوال يعد عمل النظام معاقاً، جزئياً أو كلياً، بشكل مؤقت أو دائم، حتى يمكن معرفة ما إذا كانت الإعاقة تستوجب جزاءً إدارياً أم جزاءً جنائياً بمقتضى قانونهم الداخلى.
وأخيراً، يجب أن تكون الجريمة قد ارتكبت عمداً Intentionnellement(٢)، أو بعبارة أخرى، يجب أن يكون لدى فاعل هذه الجريمة نية إحداث إعاقة جسيمة L'intention de causer une entrave grave(٣).

**المادة ٦: إساءة استخدام أجهزة الحاسب Abus de dispositif(٤):**

**النص:** (١) يجب على كل طرف أن يتبنى الإجراءات التشريعية وأية إجراءات يرى أنها ضرورية لتجريم – تبعاً لقانونه الداخلى – القيام عمداً ودون حق بما يلى:

أ – إنتاج أو بيع، أو الحصول من أجل الاستخدام، أو أستيراد أو نشر، أو أى أشكال أخرى للوضع تحت التصرف.

١ – أى جهاز، يحتوى على برنامج معلوماتى، مصمم أو مُوفق بشكل

(١) ويقابل ذلك فى المصطلح الإنجليزى Acts of interference
(٢) ويقابل ذلك فى المصطلح الإنجليزى Intentionally
(٣) ويقابل ذلك فى المصطلح الإنجليزى The intent to Seriously hinder
(٤) وردت فى الطبعة الإنجليزية Misuse of devices

أساسى لغرض ارتكاب إحدى الجرائم المنصوص عليها وفقاً للمواد من ٢-٥ السابق الإشارة إليها.

٢- كلمة المرور، أو شفرة الدخول، أو أى بيانات مماثلة تسمح بالولوج إلى كل أو إلى جزء من نظام الحاسب، بنية استخدامها لغرض ارتكاب جريمة من الجرائم المشار إليها فى المواد من ٢-٥.

ب- حيازة أى عنصر من العناصر المشار إليها فى البندين أ (١، ٢) بنية استخدامه فى ارتكاب أى جريمة من الجرائم الواردة فى المواد من ٢-٥.

(٢) هذه المادة لا يجب أن تفسر على أنها تفرض مسئولية جنائية، حينما يكون إنتاج، أو بيع، أو الحصول من أجل الاستخدام، أو الاستيراد أو النشر أو الأشكال الأخرى للوضع تحت التصرف المشار إليها فى الفقرة الأولى من هذه المادة، ليس بهدف ارتكاب جريمة، وفقاً للمواد ٢-٥ من هذه الاتفاقية، مثال ذلك، حالة الاختبار المصرح به أو حماية نظام الحاسب.

(٣) كل طرف يمكن أن يحتفظ بحقه فى تطبيق الفقرة الأولى من هذه المادة، بشرط ألا يحمل هذا التحفظ بيع أو توزيع أو وضع تحت التصرف، لأى عنصر من العناصر المشار إليها فى البندين أ (١، ٢).

التعليقات، أشارت المذكرة التفسيرية إلى أن النص يعتبر كجريمة جنائية منفصلة ومستقلة Distincte et indépendante الارتكاب عمداً Intentionnelle لأفعال غير مشروعة خاصة، ترتبط ببعض الأجهزة أو بيانات الولوج من حيث إساءة استخدامها، بغرض ارتكاب الجرائم السابق الإشارة إليها، ضد سرية وسلامة وعدم إتاحة نظم وبيانات الحاسب.

وكما يتطلب إرتكاب هذه الجرائم غالباً حيازة وسائل الولوج La Possession de moyens d'accés مثال ذلك أدوات القرصنة Outils de piratage، أو أى أدوات أخرى، فإن هناك دافعاً قوياً للحصول عليها لأغراض إجرامية، الأمر الذى يمكن أن يؤدى فى النهاية إلى خلق نوع من السوق السوداء لإنتاج وتوزيع مثل هذه الأدوات.

ومن أجل وقاية أكثر فاعلية من هذه المخاطر، فإنه يجب على قانون العقوبات أن يحظر الأفعال راجحة الخطورة من المنبع، قبل ارتكاب الجرائم المشار إليها فى المواد ٢-٥ من هذه الاتفاقية، وبهذا الخصوص فإن نص هذه المادة قد اعتمد على وسائل حديثة تبناها مجلس أوروبا بالنسبة للاتفاقية الأوروبية المتعلقة بالحماية القانونية لخدمات الولوج المشروط رقم ١٧٨(*)، وأمر الاتحاد الأوروبى رقم ٩٨/ ٨٤ بخصوص الحماية القانونية لخدمات الولوج المشروط أو النصوص وثيقة الصلة فى بعض البلدان(**).

كما تعرضت المذكرة التفسيرية لطبيعة الأجهزة محل التجريم، وهل تقتصر على الأجهزة المصممة خصيصاً لارتكاب الجرائم املعلوماتية، أم أن مظلة التجريم تمتد لتمشل الأجهزة ذات الاستخدام المزدوج المشروع وغير المشروع وفقاً لقصد الشخص من استخدامها وتوظيفه لها. فقالت:

لقد سبق أن ناقش الفقهاء مسألة ما إذا كانت الأجهزة يجب أن تقتصر على تلك المصممة فقط أو بشكل خاص من أجل ارتكاب الجرائم، وبالتالى يتم استبعاد الأجهزة ذات الاستخدام المزدوج Les dispositifs double usage.

ولكن أخذ على هذا الاتجاه أنه اتجاه ضيق للغاية Trop restrictive، إذ إنه

---

(*) وهناك مسلك مشابه سبق تبنيه فى إتفاقية جنيف لعام ١٩٢٩ والمتعلقة بتزييف العملة، ويجرم البند (a) من الفقرة الأولى الإنتاج أو البيع أو الحصول للأستخدام، أو الاستيراد أو النشر أو أية أشكال أخرى للوضع تحت التصرف لأى جها.

(د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٠٠).

(**) – ثم تبين المذكرة التفسيرية معانى بعض المصطلحات فتذكر أن:

– مصطلح النشر La diffusion ينبغى أن يمتد ليشمل كل نشاط من شأنه نقل بيانات إلى أخرين.

ومصطلح الوضع تحت التصرف Lamise à dispositior يشير إلى وضع أجهزة على الخط ليتم استخدامها بواسطة الغير، وأيضا يضم هذا المصطلح من ناحية أخرى إنشاء وتجميع الروابط بين الخطوط المتشعبة من أجل الوصول إلى هذه الأجهزة.

(المرجع نفسه – ص ١٨).

يخاطر فى الواقع بخلق صعوبات منيعة Des difficultés insurmontables[1] فيما يتعلق بتقديم الدليل L'établissement de la preuve في الإجراءات الجنائية. مما يجعل النص غير قابل للتطبيق Inapplicable، أو أنه يطبق Applicable فقط فى حالات نادرة.

كما تم أيضا استبعاد الرأى القائل بإدراج كل الأجهزة حتى تلك التى تم إنتاجها ونشرها بشكل مشروع.

ولذا لا يتبقى من أجل تطبيق العقاب كما يرى الاتجاه الثالث إلا الاعتماد على العنصر الشخصى L'élément subjectif[2] أى قصد ارتكاب جريمة معلوماتية L'intention de commettre une infraction informateique[3]، وهو نفس المسلك الذى سبق أن أخذ به فى مجال تزييف العملة La contrefaçon de monnaie[4]، وفى مقام المفاضلة بين الاتجاهات الثلاثة تبنت الاتفاقية حلاً ذا تسوية معقولة Une Sotulion de compromis raisonanble[5] وذلك بتحديد نطاق تطبيق نص المادة السادسة سالفة الذكر على الأجهزة التى يمكن موضوعياً Objectivement القول إنها مصممة أساساً من أجل ارتكاب جريمة. وبالتالى فإن هذا النص يستبعد عادة الأجهزة ذات الاستخدام المزدوج[6].

---

(١) ويقابل ذلك فى الطبعة الإنجليزية Insurmountable difficulties

(٢) ويقابل ذلك فى المصطلح الإنجليزى The subjective element

(٣) ويقابل ذلك فى المصطلح الإنجليزى The intent of committing a computer offence

(٤) ويقابل ذلك فى المصطلح الإنجليزى Money counter feiting

(٥) ويقابل ذلك فى المصطلح الإنجليزى As a reasonable compromise

(٦) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٠٣.

وجدير بالذكر أن البند (أ – ١،٠) يجرم إنتاج أو بيع، أو الحصول من أجل الاستخدام، أو الاستيراد، أو النشر، أو أية أشكال أخرى للوضع تحت التصرف، كلمة مرور D'un mot de passe، شفرة ولوج D'un code dà accès أو بيانات معلوماتية Des données informatiques مشابهة تسمح بالولوج لكل أو لجزء من نظام الحاسب.

كما أن البند (ب – ١،٠) يعتبر جريمة حيازة العناصر La possession des éléments

-/-

وفى كل الحالات، يشترط فى الجريمة أن ترتكب عمداً Intentionnellement وبدون حق Sans droit ومن أجل تجنب خطر العقاب المبالغ فيه Le Surpénalisation، حيث يتم إنتاج هذه الأجهزة وعرضها فى الأسواق لأغراض شرعية، من أجل التصدى للاعتداءات على أجهزة الحاسب Contrer des atteintes aux systemes informatiques فإنه يجب إضافة عناصر أخرى من أجل تضيق نطاق الجريمة(١).

• **العنوان الثاني: الجرائم المعلوماتية (الجرائم المتصلة بالحاسب)**

**In fractions informatiques**

تستهل المذكرة التفسيرية تقديمها لهذا العنوان بقولها: أن المواد من ٧ – ١٠ تتعلق بجرائم عادية يمكن فى الغالب أن ترتكب عن طريق الحاسب الآلى a Umoyen d'un systéme informatique، وأن غالبية الدول سبق أن قامت بتجريم هذه الجرائم العادية، وأن التشريع يمكن – وقد لا يمكن – أن يكون مرناً Soupl بطريقة كافية، من أجل أن يمتد ليشمل حالات استخدام الشبكات المعلوماتية.

على سبيل المثال: فإن قوانين بعض الدول المتعلقة بالمواد الإباحية للأطفال قد لا تنطبق على الصور الإليكترونية، وعلى ذلك فإنه من أجل وضع هذه المواد موضع التنفيذ، يجب على الدول أن تفحص قوانيها الداخلية، لتحديد ما إذا كانت تنطبق على مواقف أثمة أو متورطة Impliquant فى النظم أو شبكات الحاسب، بحيث إذا كانت الجرائم الحالية تغطى مثل هذه الأفعال، فإنه لا تكون ثمة ضرورة لتعديل الجرائم الحالية أو سن – تشريع – جرائم جديدة.

--- المشار إليها فى البند (أ – ١٠،) أو (أ–٢٠،) . كذلك فإن العبارة الأخيرة من البند (ب–١،٠) تسمح للأطراف بأن يشترطوا فى القانون الداخلى توافر بعض هذه العناصر. وعدد العناصر التى يتم حيازتها يخدم مباشرة فى إثبات النية الإجرامية. ولكل طرف أن يقرر العناصر التى ينبغى توافرها من أجل تقرير المسئولية الجنائية.

(١) المرجع نفسه.

وبالنسبة للمواد التى تحمل عنوان التزوير المعلوماتى والغش المعلوماتى، فإن هاتين الجريمتين ترتبطان ببعض الجرائم المعلوماتية، وهما نموذجان محددان للتلاعب بنظم أو بيانات الحاسب، وتدوين هاتين المادتين يشهد بحق أنه، فى بلدان كثيرة توجد مصالح قانونية تقليدية غير محمية بشكل كاف ضد الأشكال الجديدة للتدخل والهجمات[1].

**المادة ٧: التزوير المعلوماتي Falsification informatique[2]:**

**النص:** يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى، يرى أنها ضرورية لتجريم – وفقاً لقانونه الداخلى – الإدخال – الإتلاف – المحو أو الطمس العمدى، وبدون حق للبيانات المعلوماتية. الذى يتوالد عنه بيانات غير صحيحة، بقصد أخذها فى الحسبان. أو استخدامها لأغراض قانونية ما لو كانت صحيحة، بصرف النظر عما إذا كانت سهلة القراءة مباشرة وواضحة أم لا. ويمكن لأى طرف أن يشترط فى قانونه الداخلى نية الغش أو نية إجرامية مشابهة من أجل تقرير المسئولية الجنائية.

**التعليق:** تحصر المذكرة التفسيرية الغرض من هذه المادة فى إنشاء جريمة موازية لجريمة تزوير المستندات الورقية La Falsification des documents sur papier وتهدف هذه الجريمة إلى استكمال أوجه النقص التى تعترى قانون العقوبات بالنسبة للتزوير التقليدى La Falsification classique، الأمر الذى يتطلب سهولة القراءة المرئية للإقرارات المتضمنة فى المحرر، والتى لا تنطبق على البيانات المسجلة على دعامة إليكترونية، والتلاعب بالبيانات المسجلة له قوة دامغة، يمكن أن تكون لها نفس النتائج الوخيمة للأفعال التقليدية للتزوير إذا تم إيقاع الطرف الثالث فى الغلط[3].

(١) المرجع نفسه – ص ١٠٥.
(٢) يقابل ذلك فى النص الإنجليزى Computer related - forgery
(٣) د/ عمر محمد بن يونس – الاتفاقية الأوروبية للجريمة الافتراضية – مرجع سابق – ص ٨٥. (بالنسبة لنص الاتفاقية بالإنجليزية)، د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٠٧ (بالنسبة لنص الاتفاقية بالفرنسية).

والتزوير المعلوماتي يتكون من خلق Créer أو تعديل غير مصرح به Modifier sans autorisation للبيانات المسجلة، بطريقة من شأنها أن تحوز هذه البيانات قيمة دامغة مختلفة عن سياق المعاملات القانونية، والتي تكون مؤسسة على صحة المعلومات المستخرجة من خلال هذه البيانات، وبالتالي يمكن أن تكون موضوعاً لخداع D'une tromperie المصالح القانونية المحمية. والمصلحة المشمولة بالحماية القانونية هنا هي الأمن والثقة في البيانات المخزنة، وإمكانية تشغيل البيانات الإلكترونية، والتي يمكن أن تكون بها عواقب على العلاقات القانونية.

– ويجب أن يلاحظ أن مفهوم التزوير يتنوع Varie كثيراً من دولة إلى أخرى، فهناك مفهوم يكون مؤسساً على الصحة L'authenticité بالنسبة لكاتب الوثيقة، في حين أن بعض المفاهيم الأخرى ترتكز على صدق Lavéracité المعلومات المتضمنة في الوثيقة محل البحث.

وعلى ذلك فإن الإدخال غير المصرح به للبيانات الصحيحة وغير الصحيحة يخلق موقفاً يناظر عمل محرر مزور، كذلك فإن العمليات اللاحقة للإتلاف كالتعديلات أو التغييرات الجزئية، والمحو والطمس كواقعة حفظ وإخفاء بيانات، كل أولئك يناظر بشكل عام تزوير محرر صحيح ومصطلح لأغراض قانونية à des fins légales ينطبق أيضاً على المعاملات والمحررات القانونية التي تكون قانوناً متوافقة.

**المادة ٨: الغش المعلوماتي Fraude informatique(١):**

**النص:** يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم – تبعاً لقانونه الداخلي – عمداً ودون حق، التسبب في إحداث ضرر مالي للغير عن طريق:

أ – الإدخال، الإتلاف، المحو، أو الطمس لبيانات الحاسب.

(١) يقابل ذلك في النص الإنجليزي Computer - related fraud

ب- كل شكل للاعتداء على وظيفة الحاسب، بنية الغش - نية إجرامية مشابهة - من أجل الحصول - دون حق - على منفعة اقتصادية له أو للغير.

التعليق: تشير المذكرة التفسيرية إلى أنه مع حدوث الثورة التكنولوجية La réuolution technologique[1] تضاعفت إمكانيات ارتكاب جرائم اقتصادية، كالغش - وبالأخص - النصب ببطاقات الائتمان، كما أن الأصول الممثلة أو المتداولة عن طريق النظم المعلوماتية، كالأموال الإليكترونية أو الودائع أصبحت هدفاً للتلاعبات بنفس الأشكال التقليدية للملكية.

وهذه الجرائم تتكون بشكل أساسي من خلال التلاعبات بمدخلات النظام، بمعنى تغذية الحاسب ببيانات غير صحيحة، أو من خلال تلاعبات في البرامج، أو من خلال تدخلات أخرى في معالجة البيانات. والهدف المتوخى من هذه المادة تقرير الجزاء الجنائي المستحق لكل تلاعب تعسفي، في سياق المعالجة الآلية للبيانات يكون من شأنه نقل غير شرعي للملكية(*).

**• التلاعبات المعلوماتية الاحتيالية :-**

**Les manipulations infarmotiques frauduleuses:[2]**

تكون مجرمة إذا سببت مباشرة للغير ضرراً اقتصادياً أو مادياً، أو أن يكون الجاني قد نفذ الجريمة بنية الحصول على منفعة اقتصادية غير مشروعة له أو للغير، ومصطلح الضرر الاقتصادي أو المادي يتصل بمفهوم واسع جداً، يشمل النقود والأشياء المادية وغير المادية ذات القيمة الاقتصادية ويجب أن ترتكب الجريمة بدون حق Sans droit كما يجب أن يكون الحصول على المنفعة الاقتصادية دون حق أيضاً.

---

(١) يقابل ذلك في النص الإنجليزي The Technological revolution

(*) Un transpert illicite de proprété.

(٢) يقابل ذلك في الطبعة الإنجليزية The computer fraud manipulations

وبالتالى فإن الممارسات التجارية العادية الشرعية، التى يتم تنفيذها بنية الحصول على منفعة اقتصادية لا تعد جريمة فى حكم هذه المادة، لأن الأفراد يتصرفون فى نطاق حقهم القانونى[1].

مثال ذلك: الأنشطة التى تتم بمقتضى عقد صحيح Un contrat en bonne بين طرفين تكون مشروعة. مثال ذلك النشاط الذى يكون محوره تعطيل Désactiver[2] موقع شبكة Un site web وفقاً لبنود العقد محل البحث.

كذلك يجب أن ترتكب الجريمة عمداً Intetionnellement، والعنصر العام للقصد ينطبق على التلاعب، أو التدخل المعلوماتى الذى يسبب ضرراً اقتصادياً أو مادياً للغير. وعلاوة على ذلك تتطلب الجريمة نية خاصة هى نية الغش أو (نية غش خاصة Une intention frauduleuse spécifique)[3] أو بتعبير آخر نية غير أمينة أو غير شريفة Malhonnête بغرض الحصول على منفعة اقتصادية لنفسه – المتهم المعلومات – أو للغير.

وبمفهوم المخالفة، فإن الأنشطة التجارية المتعلقة بالمنافسة La concurrence، والتى يمكن أن تسبب ضرراً اقتصادياً لشخص وتحمل منفعة لآخر، بيد أنه لا يتم ممارستها من خلال نية غش أو نية غير أمينة، فإنها لا تشكل جريمة فى حكم المادة الثامنة. مثال ذلك: استخدام برامج جمع المعلومات L'utilisation de programmes de collecte d'informations[4] من أجل المنافسة على الإنترنت، حتى لو كان غير مصرح به عند زيارة الموقع بواسطة صائد المعلومات "Bot"[5].

---

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١١٤.

(٢) ويقابل ذلك فى المصطلح الإنجليزى Disabling بمعنى تعطيل أى منع نشاط معين عن التنفيذ، مثلا كون جهاز معين فى وضع غير متاح للتشغيل (على يوسف على مرجع سابق – ص ٢١٩).

(٣) ويقابل ذلك فى المصطلح الإنجليزى A specific fraudulent intent

(٤) ويقابل ذلك فى الطبعة الإنجليزية The use of information gathering programs

(٥) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١١٥.

• **العنوان الثالث: الجرائم المتصلة بالمحتوي**

**Infractions se rapportuat au contenu**

هذا العنوان يغطى الجرائم المرتبطة بالمحتوى، بمعنى الإنتاج أو النشر غير المشروع للمواد الإباحية الطفولية، عبر النظم المعلوماتية، والذى يمثل نماذج تنفيذ الجريمة، الأكثر خطورة، والذى بدأ فى الظهور حديثاً(١).

**المادة ٩: الجرائم المتصلة بالمواد الإباحية للأطفال:**

(٢)**Infractions se rapportant à la pornographie enfantine**

النص: ١- يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية، لتجريم – تبعاً لقانونه الداخلى – السلوكيات التالية إذا أرتكبت عمداً ودون حق:

أ – إنتاج مواد إباحية طفولية بغرض نشرها عبر نظام معلوماتى.

ب– تقديم أو إتاحة مادة إباحية طفولية عبر نظام معلوماتى.

جـ– النشر أو النقل لمادة إباحية طفولية عبر نظام معلوماتى.

د – واقعة التزود أو تزويد الغير بمادة إباحية طفولية عبر نظام معلوماتى.

هـ– حيازة مادة إباحية طفولية فى نظام معلوماتى أو فى أى وسيلة لتخزين البيانات المعلوماتية.

٢– توخياً لأغراض الفقرة الأولى عاليه، فإن مفهوم المادة الإباحية الطفولية يشمل كل مادة إباحية تمثل بطريقة مرئية:

---

(١) مما تجدر الإشارة إليه أنه أثناء قيام اللجنة بوضع مسودة الاتفاقية – محل البحث – ناقشت مدى إمكانية إدراج جرائم أخرى تتعلق بالمحتوى، مثال ذلك نشر دعاية عنصرية عبر نظم الحاسب أو النظم المعلوماتية، بيد أن اللجنة لم تكن فى وضع يسمح لها بالوصول إلى موافقة جماعية أو توافق بخصوص تجريم مثل هذا السلوك وقد قررت اللجنة أن تكلف اللجنة الأوروبية للمشاكل الجنائية، باقتراح اعداد بروتوكول أضافى يدرج بهذه الاتفاقية الحالية.

(٢) يقابل ذلك فى النص الإنجليزى Offences related to child pornography

أ – حدث يقوم بسلوك جنسى صريح.

ب- شخص يبدو كأنه حدث يقوم بسلوك جنسى.

جـ- صور حقيقية تمثل حدثاً يقوم بسلوك جنسى صريح.

٣- توخياً لأغراض الفقرة الثانية عاليه، فإن مصطلح «حدث» يشمل كل شخص عمره أقل من ١٨ عاماً. ومع ذلك فإنه يمكن لأى طرف أن يستوجب حداً عمرياً أقل، بشرط ألا يقل عن ١٦ عاماً.

٤- كل طرف له الحق فى عدم تطبيق كلياً أو جزئياً الفقرات (١ – د، هـ)، (٢ – ب، ج).

التعليق: تشير المذكرة التفسيرية إل أن المادة التاسعة المتعلقة بالمواد الإباحية الطفولية La pornographie enfantine[1] تسعى إلى تدعيم الإجراءات التى تحمى الأطفال خاصة حمايتهم ضد الاستغلال الجنسى L'exploitation sexuelle[2]، من خلال تحديث قانون العقوبات، بطريقة أكثر فاعلية، تشتمل على استخدام نظم الحاسب الآلى فى أطار ارتكاب الجرائم الجنسية ضد الأطفال[3].

---

(١) يقابل ذلك فى الطبعة الإنجليزية Child pornography

(٢) ويقابل ذلك فى المصطلح الإنجليزى Sexual exploiIation

(٣) تستجيب هذه المادة لقلق La préoccupation رؤساء الدول والحكومات أعضاء مجلس أوروبا Le conseil de l'europe والذى تم التعبير عنه فى اجتماع القمة الثانى 2e sommet فى ستراسبورج ١٠-١١ أكتوبر ١٩٩٧.

كما تتوافق هذه المادة أيضاً مع تطور عالمى Une évolution internationale يسعى إلى حظر المواد الإباحية الطفولية، كما تأكد حديثاً من خلال تبنى البروتوكول الاختيارى Le Pro-tocole Facultatif لاتفاقية الأمم المتحدة لحقوق الطفل La convention des nations unies relative aux droits de l'enfant المرتبط بالآتى:

- بيع الأطفال La vente d'enfants
- ودعارة الأطفال La prostitution des enfants
- والمواد الإباحية الآثمة للأطفال La pornographie impliquant des enfants

للمزيد يراجع: د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢١.

وبالرغم من أن فكرة إدراج فكرة إدراج هذا النشر - غير المشروع للمواد الإباحية الطفولية - بوصفه جريمة جنائية، قد وجد دعما على نطاق واسع، إلا أن بعض الوفود أبدت تحفظات حقيقية، بإثارتها لمبدأ حرية التعبير La Liberte d'expression(*).

ويتوافق نص ا لمادة التاسعة مع التوجه الدولي الساعي إلى حظر دعارة الأطفال، كذلك تتوافق هذه المادة أيضاً مع المبادرة الحديثة للجنة الأوروبية المتعلقة بمكافحة الاستغلال الجنسي للأطفال والمواد الإباحية الطفولية رقم ٨٥٤ لسنة ٢٠٠٠.

وتجرم هذه المادة مختلف جوانب الإنتاج والحيازة والنشر للمواد الإباحية الطفولية، مع ملاحظة أن معظم الدول تجرم بالفعل الإنتاج التقليدي والنشر المادي للمواد الإباحية الطفولية، ولكن بما أن استخدام شبكة الإنترنت يتسع أكثر فأكثر باعتبارها أداة رئيسية للإتجار في هذه المواد، فإن ذلك أدى إلى وجوب وضع نصوص خاصة في الاتفاقيات القانونية الدولية، لمكافحة هذا الشكل الجديد من الاستغلال الجنسي للأطفال وتعريضهم للخطر كلية بصفة أساسية.

- وبالنسبة لتعبير مادة إباحية طفولية الوارد في الفقرة الثانية من المادة التاسعة، فإنه يجب أن يتم تفسيره وفقاً لضوابط القانون الداخلي المتعلقة بتصنيف هذه المواد، كأن تكون فاحشة أو غير متفقة مع الآداب العامة، أو أنها تدخل تحت عنوان آخر لفعل المنحرفين.

- وتعبير السلوك الجنسي الصريح يتحدد بواحد أو أكثر من السلوكيات الحقيقية أو المصطنعة مثل:

---

(*) بالنظر إلى تعقد هذه المسألة، قررت اللجنة المشكلة لوضع مسودة الاتفاقية الأوروبية، أن تكلف اللجنة الأوروبية للمشاكل اللجنائية (D.P.C.).

- Comité européen pour problémes criminels.

باقتراح إعداد بروتوكول إضافي يُدرج بالاتفاقية الحالية، يعالج هذه المشكلات.

أ – العلاقات الجنسية.

بما فى ذلك أعضاء تناسلية – مع أعضاء تناسلية، أو اعضاء تناسلية – فميه، أو أعضاء تناسلية – شرجية، أو شرجية – فمية.

وذلك بين أحداث أو بين حدث وشخص راشد من نفس الجنس أو من جنسين مختلفين.

ب– إتيان الحيوانات.

جـ– الاستمناء أو ممارسة العادة السرية.

د – الممارسة السادية الماسوشية أثناء الجماع الجنسى.

هـ– عرض شهوانى للأعضاء الجنسية أو لمنطقة العانة، بالنسبة للحدث.

وفى كل الحالات، لا يدخل فى الحسبان كون السلوك المصور حقيقياً أم مصطنعاً.

- وبالنسبة لتعبير (حدث) فيما يتعلق بالمواد الإباحية الطفولية عموماً، فإن الفقرة الثالثة من المادة التاسعة مقدمه بأنه كل شخص عمره أقل من ١٨ سنة، وفقاً لتعريف كلمة طفل فى المادة الأولى من اتفاقية الأمم المتحدة المتعلقة بحقوق الطفل، وقد أخذ فى الحسبان أن بعض الدول تتطلب تحديداً للعمر أقل فى التشريع الوطنى المتعلق بالمواد الإباحية الطفولية، فإن العبارة الأخيرة من الفقرة الثالثة تسمح للأطراف أن يشترطوا حداً عمرياً مختلفاً، شريطة ألا يقل عن ١٦ عاماً.

وبالنسبة للركن المعنوى فى هذه الجريمة، فإن المادة التاسعة تدرج أنواعاً مختلفة للأفعال غير المشروعة Actes illicites المرتبطة بالمواد الإباحية الطفولية. والتى كما فى المواد ٢–٨ يلتزم الأطراف بتجريمها إذا ارتكبت «عمداً» Intentionne llement. وبمقتضى هذا المعيار فإن الشخص لا يمكن أن يكون مسئولاً إلا إذا كان لديه نية Intention تقديم أو إتاحة أو نشر أو نقل أو انتاج أو حيازة مادة إباحية طفولية(١).

---

(١) المرجع السابق – ص ١٢٩،

• **العنوان الرابع: الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة:**

**Infrctions lieés aux atteintes à la proprité intellectuelle et aux droits connexes**

يحدد العنوان الرابع «الجرائم المعلقة بالاعتداء على الملكية الفكرية والحقوق المجاورة أو المرتبطة بها»، وقد نصت الاتفاقية على هذه النوعية من الجرائم؛ وذلك لأن الانتهاكات الواقعة على الملكية الفكرية هى أحد أشكال الإجرام المعلوماتى الأكثر شيوعاً، والذى بازدياد نسبته يزداد قلق وأنشغال العالم بأسره، بهذا التيار الإجرامى المتقدم.

**النص: المادة ١٠ - الجرائم المتصلة بالاعتداءات الواقعة على الملكية الفكرية والحقوق المجاورة(١):**

١- يجب على كل طرف أن يتبنى الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية لتجريم - تبعاً لقانونه الداخلى - انتهاكات الملكية الفكرية المعرفة فى قانون ذلك الطرف، وفقاً للالتزامات التى تم التوقيع عليها فى ظل الاتفاقية العالمية لحق المؤلف الموقعة فى باريس فى ٢٤ يوليو ١٩٧١، واتفاقية برن لحماية الأعمال الأدبية والفنية، واتفاقية المنظمة العالمية للملكية الفكرية (OMPI) - بأستثناء أى حق معنوى ممنوح بواسطة هذه الاتفاقيات - إذا ما ارتكبت هذه الأفعال عمداً، وعلى نطاق تجارى وبواسطة نظام معلوماتى.

٢- يجب على كل طرف يتبنى الإجراءات التشريعية، وأيه إجراءات أخرى، يرى أنها ضرورية من أجل تجريم - تبعاً لقانونه الداخلى - انتهاكات الحقوق المجاورة المعرفة فى قانون هذا الطرف، وفقاً للالتزامات التى تم التوقيع عليها فى ظل الاتفاقية الدولية لحماية الفنانين، المؤدين أو العازفين

---

(١) وقد ورد النص الإنجليزى لهذه المادة.

Offences related to infringeménts of copyright dand related rights.

ومنتجى الصوتيات ومنظمات البث المبرمة فى روما (أتفاقية روما)، واتفاقية الجوانب التجارية لحقوق الملكية الفكرية واتفاقية المنظمة الدولية للملكية (OMPI) بالنسبة للأداء العزف، والبث - بأستثناء أى حق معنوى منصوص عليه بواسطة هذه الاتفاقيات إذا تم ارتكاب هذه الأفعال عمداً، وعلى نطاق تجارى، أو بواسطة نظام معلوماتى.

٣- يمكن لأى طرف، فى ظل ظروف محدودة للغاية، أن يحتفظ بالحق فى عدم تطبيق المسئولية الجنائية، بالنسبة للفقرتين الأولى والثانية من هذه المادة، بشرط توافر طرق أخرى فعالة وجاهزة، وأن لا يكون فى هذا التحفظ ما يحمل اعتداء على الالتزامات الدولية المفروضة على هذا الطرف، فى تطبيق الاتفاقيات الدولية المشار إليها فى الفقرتين الأولى والثانية من هذه المادة.

التعليق[1]: تنبه المذكرة التفسيرية إلى أن انتهاكات حقوق الملكية الفكرية Les atteintes aux droits de proprieté، وعلى وجه الخصوص حق المؤلف Le droit d'auteur تعتبر من بين الجرائم الأكثر انتشاراً على الإنترنت، الأمر الذى يهم كلاً من أصحاب أو حائزى حق المؤلف (حقوق التأليف)، ومتخصصى الشبكات المعلوماتية.

- إن إعادة إنتاج وبث الأعمال المحمية عبر الإنترنت دون موافقة حائز حق المؤلف هو أمر شائع للغاية، وهذه الأعمال المحمية تشمل على وجه الخصوص:

الأعمال الأدبية والتصويرية والموسيقية والسمعية بصرية، وجدير بالذكر أن السهولة التى من خلالها يمكن عمل نسخ غير مصرح بها عن طريق التكنولوجيا الرقمية، والنطاق الذى بمقتضاه يتم إعادة الإنتاج والتوزيع عبر الشبكات الإليكترونية، كل أولئك فرض ضرورة وضع نصوص تشتمل على جزاءات جنائية، وتفرز التعاون الدولى فى هذا المجال.

---

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١٣٤، د/ عمر محمد بن يونس - المرجع السابق - ص ٩٩.

- ويمقتضى الأصول المشار إليها فى هذه المادة، فإن كل طرف يكون ملزماً بتجريم الانتهاكات العمدية Les atteintes déliberées على الملكية الفكرية، وعلى الحقوق المتصلة، والتى يشار إليها تحت عنون الحقوق المجاورة Les droits connexes، إذا كانت هذه الانتهاكات قد تم ارتكابها عن طريق نظام معلوماتى، وعلى نطاق تجارى.

وإذا كانت الفقرة الأولى من هذه المادة تقرر جزاءات جنائية ضد انتهاكات الملكية الفكرية المرتكبة بأستخدام نظام معلوماتى، مع ملاحظة أن انتهاك حق المؤلف هو جريمة بالفعل فى كل الدول تقريباً، فإن الفقرة الثانية من هذه المادة تتعامل مع انتهاكات الحقوق المجاورة، التى يتم ارتكابها بأستخدام نظام معلوماتى، وانتهاكات الملكية الفكرية والحقوق المجاورة أو المتصلة بها تتطابق مع التعريفات التى يمنحها التشريع الداخلى بكل طرف، بغرض تنفيذ الالتزامات التى تم التوقيع عليها بمقتضى معاهدات دولية معينة،

وإذا كان يجب على كل طرف أن يجرم هذه الانتهاكات، غير أن التعريف الدقيق La définition précise لهذه الجرائم فى القانون الداخلى يمكن أن يكون متغيراً ومتنوعاً Varier من دولة لأخرى. ومع ذلك فإن الألتزام بالتجريم الناتج عن الاتفاقية لا يغطى من أنتهاكات الملكية الفكرية غير تلك المنصوص عليها صراحة فى المادة ١٠، وبالتالى يتم استبعاد انتهاكات حقوق براءات الأختراع des brevets، والعلامات التجارية des marques.

وبالنسبة للركن المعنوى للجرائم المرتبطة بحق المؤلف والحقوق اللصيقة بها فإنة يجب أن ترتكب délibérement من أجل تقرير المسئولية الجنائية.

وبالنسبة للفقرة الثالثة من هذه المادة، فإنها تسمح للأطراف بألا يطبقوا المسئولية الجنائية فى الفقرتين الأولى والثانية فى ظروف محددة للغاية، مع وجود طرق أخرى فعالة وبالأخص الاجراءات ذات الطابع المدنى أو الإدارى التى تكون متاحة.

## المبحث الثاني

## إتفاقية الجرائم المعلوماتية (المجلس الأوروبي)

## (The Cyber Crime Convention)

تعد إتفاقية الجرائم المعلوماتية، من أحدث الاتفاقيات المكافحة للجريمة المعلوماتية على المستوى الدولي، وهي صادرة عن المجلس الأوروبي، حيث وقعت ٣٢ دولة عليها، وصادقت ٩ دول على أنفاذ بنودها، وقد دخلت إلى حيز النفاذ اعتباراً من أول يوليو ٢٠٠٤، فيما تسعى العديد من الدول إلى الانضمام إليها. وتعتبر إتفاقية الجرائم المعلوماتية هي الاتفاقية الوحيدة الملزمة في هذا المجال(*).

- **كيفية الأنضمام إلي الإتفاقية:**

إذا أرادت احدى الدول الانضمام للاتفاقية، يمكنها الاتصال بأمانة المجلس الأوروبي (مكتب المعاهدات التابع للمجلس الأوروبي - إدارة مشكلات الجريمة)، وبناء على طلب الدولة المعنية، تقوم أمانة المجلس الأوروبي بطرح الأمر على لجنة وزراء المجلس الأوروبي المسئول عن دعوة هذه الدولة للأنضمام كطرف في الاتفاقية.

- **الجرائم المنصوص عليها بالاتفاقية:**

- الجرائم المرتكبة ضد سرية وتكامل وتوافر البيانات أو نظم الكمبيوتر. (مثل: التدخل، الإختراق، التعدى على أجهزة الكمبيوتر).
- الجرائم المتصلة بالمحتوى.

---

(*) جدير بالذكر أن السيد/ جيانلوكا إيسبيسيتو Gianluca Esposito (رئيس قسم الجرائم الإقتصادية) بالمجلس الأوروبي، وقد حضر المؤتمر الدولي السادس للجرائم المعلوماتية المنعقد بأكاديمية الشرطة - القاهرة - الفترة ١٣: ١٥ ابريل ٢٠٠٥. حيث قدم نموذجاً متكاملاً عن اتفاقية الجرائم المعلوماتية الصادرة برعاية المجلس الأوروبي.

- الجرائم التى تتضمن إنتهاكاً لحقوق الملكية الفكرية، وما يتصل بها من حقوق.

وتتبع الاتفاقية مجموعة من الأساليب التحقيقية، التى يمكن من خلالها تغطيت الجرائم المتصلة بالاتفاقية، واية جرائم أخرى ترتكب من خلال/ أو على/ أو ضد نظم الكمبيوتر. كما أوضحت الاتفاقية أنه يمكن إستخدام الأدوات التحقيقية فى الحالات التى يرتكب فيها الجرم بواسطة نظام كمبيوتر، أو التى يكون فيها الدليل على الجرم المرتكب إلكترونياً.

- **من الأساليب التحقيقية في جرائم المعلوماتية:**

- أسلوب تفتيش وضبط أنظمة الكمبيوتر: وتهدف هذه الوسيلة إلى تحديث التشريعات، وتحقيق التواءم - الإندماج - اللازم فيما بينها، وذلك فى مجال تفتيش وضبط البيانات المخزونة على اجهزة الكمبيوتر، فيما يتصل بأحد التحقيقات الجنائية أو إحدى القضايا المحددة(*).

---

(*) من الأساليب التحقيقية الأخرى التى تضمنتها الاتفاقية:

- **أسلوب الحفظ السريع لبيانات الكمبيوتر المخزونة:**

وينطبق ذلك على البيانات المخزونة التى تم جمعها وحفظها فعلياً بمعرفة حائز البيانات.
وينطبق هذا الأسلوب - فقط - فى الأحوال التى تتوافر فيها بيانات الكمبيوتر فعلياً ويتم تخزينها على أحد الأجهزة.
ويتميز هذا الأسلوب بأنه أسلوب تحقيق جديد وهام، وبخاصة فيما يتعلق بالجرائم التى ترتكب عبر شبكة الأنترنت، وذلك نظراً لإمكانية تعرض بيانات الكمبيوتر للمحو أو التلاعب، والخطر المحتمل المتمثل فى إمكانية فقدان الدليل.

- **أسلوب الأمر بإصدار نسخة من البيانات:**

يُمكن هذا الأسلوب السلطات المختصة - المعنية بجرائم المعلوماتية - من اجبار الشخص على تقديم بعض بيانات الكمبيوتر المخزونة المحددة، أو أحد عناوين ISP المعنية، التى تسهم فى التوصل إلى معلومات حول المشترك وتنطبق هذه الأوامر - فقط - فى حالة البيانات المخزونة والموجودة بالفعل.

وتجدر الإشارة إلى أنه يتطلب التفتيش والضبط فى بيئة الإنترنت عناية خاصة، وذلك نظراً لأن:

- البيانات من خلال الانترنت تكون فى صورة غير ملموسة.
- على الرغم من إمكانية قراءة البيانات على الكمبيوتر، إلا أنه من غير الممكن ضبطها ونقلها كما هو الحال بالنسبة للدليل المادى(*).

● **إجراءات توسيع نطاق الانضمام للإتفاقية:**

تبنى منفذوا الاتفاقية فى نطاق المجلس الأوروبى بعض الخطوات الرامية إلى زيادة فاعلية الاتفاقية فى محيط المجتمع الدولى، من هذه الخطوات:

- تبنى اجتماع (ابيك) – بانكوك سنة ٢٠٠٢ – تشريعاً لمكافحة الجريمة المعلوماتية ينسق وأحكام إتفاقية الجريمة المعلوماتية (الأوروبية).
- أوصى اجتماع منظمة الدول الأمريكية (نيويورك – سنة ٢٠٠٤) بتقييم مدى الاستفادة المتحققة من إعمال المبادئ المتضمنة فى اتفاقية المجلس الأوروبى حول الجريمة المعلوماتية، ومدراسة إمكانية الإنضمام إليها.
- CEO – سبتمبر ٢٠٠٤: مؤتمر الجريمة المعلوماتية فى ستراسبورج، وقمة رؤساء الدول والحكومات المنعقد فى (وارسو – مايو ٢٠٠٥)، والاشارة إلى اتفاقية الجرائم المعلوماتية (الأوروبية)، وحث المجتمع الدولى على سرعة الأنضمام – والاستفادة والمدارسة – للاتفاقية ومحتواها.

---

(*) من الأساليب التحقيقية التى صاغتها الاتفاقية للتغلب على صعوبة ضبط البيانات على الكمبيوتر، والتعويل عليه كدليل مثل الدليل المادى.

- **أسلوب الجمع الفوري لبيانات الكمبيوتر. ويعتمد على:**
- الجمع الفورى لبيانات النقل – ويعنى بالبيانات المتعلقة بأحد الاتصالات التى تتم بواسطة نظام الكمبيوتر.
- إعتراض بيانات المحتوى / إعتراض محتوى الاتصال، سواء الرسالة أو المعلومة المنقولة.

## الباب الثاني

# الحماية الإجرائية للمعلوماتية

## تمهيد:

الجريمة المعلوماتية مثل غيرها من الجرائم لها أركانها وعناصرها، وتسير الدعوى الجنائية بالنسبة لها بذات المراحل التي تسير فيها الدعوى الجنائية في الجرائم العادية (التقليدية)(*) كالقتل والسرقة والضرب والتزوير.

وإذا كان الاعتراف يأخذ به في الاثبات - إذ لم يعد هو سيد الأدلة - يليه شهادة الشهود، ثم القرائن والأدلة والآثار الناجمة عن النشاط الاجرامي بما لذلك من دور في إثبات الجريمة العادية - وكذلك الجريمة المعلوماتية - وكشف حقيقتها ومرتكبها، وهي أمور عديدة تعين المحقق الجنائي على ضبط الواقعة وإعمال القانون وبسط العدالة.

وإذا صدق ما سبق ذكره بالنسبة للجرائم المنصوص عليها في القانون، فإن قواعد هذا القانون تبدو قاصرة إزاء ملاحقة مرتكب الجريمة المعلوماتية، مما حدا بالبعض إلى القول بأن قواعد قانون العقوبات (الإجراءات) التقليدي تواجه تحديات إزاء مواجهة الجريمة المعلوماتية، وتبدو قاصرة عن مواجهة العديد من الأفعال التي تهدد مصالح إجتماعية واقتصادية ارتبطت بظهور وانتشار جهاز الحاسب الآلي وشبكة المعلومات الدولية (إنترنت)[1].

ولقد كان ظهور الجريمة المعلوماتية عاملاً حاسماً في قيام الكثير من الدول بسن تشريعات جديدة أو تعديل تشريعاتها القائمة لمواجهة الجريمة المعلوماتية، إلا أن المشرع في البلدان العربية لم يتدخل جدياً - بعد - لمواجهة هذا النوع من

---

(*) يقصد بالجرائم التقليدية: كل الجرائم المنصوص عليها في التشريعات العقابية، والقوانين المكملة لها، ما خلا جرائم الحاسب الآلي أو الجرائم المعلوماتية، أو الجرائم الافتراضية المستحدثة نتيجة التقنيات الحديثة.

(١) د/ غنام محمد غنام - عدم ملائمة القواعد التقليدية في قانون العقوبات لمكافحة جرائم الكمبيوتر - بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت - كلية الشريعة والقانون - جامعة الإمارات - دولة الإمارات العربية المتحدة - مايو عام ٢٠٠٠ - ص ١.

الجرائم بنصوص خاصة، فضلاً عن أن القضاء لم يواجه بعد مشكلات قانونية تتعلق بحماية المعلومات والبرامج التى تخص الكمبيوتر(١).

وإزاء هذا القصور التشريعى، وندرة التطبيق القضائى، يبرز كأمر واقع مسألة صعوبة جمع الاستدلالات والأدلة فى الجريمة المعلوماتية، وأيضاً تطبيق الإجراءات الجنائية التقليدية، حتى يمكن تحقيق عناصر الجريمة والتصرف فيها مثل الجرائم الأخرى.

إذ أن هذه النوعية من الجرائم توجد فى بيئة لا تعتمد التعاملات فيها - أصلاً - عى الوثائق والمستندات المكتوبة، بل على نبضات إليكترونية غير مرئية لا يمكن قراءتها إلا بواسطة الحاسب، والبيانات التى يمكن استخدامها كأدلة ضد الفاعل يمكن فى جزء من الثانية العبث بها أو محوها بالكامل(٢).

لذلك وبعد أن أصبح المجتمع المعلوماتى حقيقة واقعة، وتعتمد المجتمعات المعاصرة فى تسيير شئونها على تقنيات الحاسبات والمعلومات، فإنه يتعين على أجهزة العدالة الجنائية - مع تقليص الدور التقليدى للوثائق فى الإثبات، والزيادة المطردة فى كم المعلومات المنتجة أو المعروضة فى أوعية (لا ورقية بل مستحدثة) - أن تتعامل فى ممارستها لحق المجتمع فى الدفاع عن كيانه ضد الإجرام مع أشكال مستحدثة من الأدلة غير المادية، وذلك فى مجال الأثبات

---

(١) المرجع السابق - ص ٢.

ويذكر فى هذا الخصوص صدور بعض القوانين التى تناولت جانب من المعلوماتية مثل:

- قانون التجارة الإليكترونية فى تونس سنة ٢٠٠٠.
- وقانون التجارة الإليكترونية فى إمارة دبى رقم ٢ لسنة ٢٠٠٢.
- وقانون التوقيع الإليكترونى المصرى رقم ١٥ لسنة ٢٠٠٤.

حيث تضمنت جميعها نصوصاً تواجه الجريمة المعلوماتية.

ويضيف الباحث: ان هذا التناول للمشرع فى هذه البلدان يحمد عليه، ولكنه تناول جزء يسير فى النظم المعلوماتية بالتشريع، بينما الكم الكثير من التدفق المعلوماتى، مازال ينتظر الحماية القانونية.

(٢) د/ عبد الفتاح بيومى حجازى - مبادئ الإجراءات الجنائية (فى جرائم الكمبيوتر والإنترنت) - دار الفكر الجامعى - الاسكندرية - ط أولى - سنة ٢٠٠٦ - ص ٥٤.

الجنائي[1]. وهو ما يفرض على الفكر الشرطي – سلطة جمع الاستدلالات – السعي دوماً إلى:

اولاً: تطوير أساليب كشف الجريمة المعلوماتية، والوسائل المستخدمة في عمليات البحث الجنائي والتحقيق المعلوماتي.

ثانيا: تحديث الأساليب الإجرائية المتبعة لجمع الأدلة في الجرائم المعلوماتية، على النحو الذى يكفل استجابتها بشكل كاف – وبغير أن تتعرض حقوق الأفراد وحرياتهم للخطر – عند الإثبات في مجال الجريمة المعلوماتية، التي لا تعترف بالمكان من حيث آثارها، وتستعصى على القواعد التقليدية في قانون الإجراءات الجنائية[2].

**تقسيم:**

وفي ضوء عرض الحماية الإجرائية للمعلوماتية، سوف تنقسم الدراسة إلى فصلين هما:

**الفصل الأول - الحماية الإجرائية القانونية للمعلوماتية.**

**الفصل الثاني - الحماية الفنية للمعلوماتية.**

ويسبق ذلك عرض لمفهوم الحماية الإجرائية، كنقطة أولى تعد الأساس الذى تشيد عليه الحماية الإجرائية للمعلوماتية، ثم عرض للشرعية الإجرائية للمعلوماتية، حيث تمثل الشرعية حجر الزاوية في الإجراءات القانونية التي يباشرها مأمور الضبط في سبيله لمكافحة الاجرام المعلوماتي والغاية التي تسعى السلطة القضائية للتأكد من الالتزام بفحواها ومضمونها من جانب ممثلوا السلطة التنفيذية، إنها القبلة التي ينشدها المجتمع المعلوماتي المتحضر.

---

(١) د/ هشام محمد فريد رستم – أصول التحقيق الجنائي والفني (اقتراح بإنشاء آلية عربية موحدة للتدريب التخصصي) – بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت بجامعة الإمارات – دولة الإمارات العربية المتحدة – سنة ٢٠٠٠ – ص ٢١.

(٢) د/ هلالي عبد اللاه أحمد – بحث بعنوان: حجية المخرجات الكمبيوترية – مؤتمر القانون والكمبيوتر – سابق الاشارة إليه – ص ٢.

**أولاً: مفهوم الحماية الإجرائية:**

يعد القانون الجنائى فرع من فروع القانون العام الذى يضم بين ضفتيه نوعين من القواعد القانونية:

الأولى – تسمى القواعد الموضوعية.

والثانية – تسمى القواعد الإجرائية.

وتهدف القواعد الموضوعية – وهى ما تعرف بقانون العقوبات – إلى بيان الجرائم والعقوبات المقررة لهم، فهى تضع قيداً على سلوك المواطنين وتنذر بالعقاب من يتعدى عليها، وبهذا المعنى يكون قانون العقوبات من أهم فروع القانون، بل هو من أقدمها تاريخاً ذلك أن الشرائع القديمة فى معظمها نصوصاً جزائية. ولكى تكون العقوبة أداة رقى وأصلاح يجب أن تتناسب مع مدى خطورة الجُرم والمجرم فى نظر المجتمع، وتضمن بتناسبها واعتدالها تطبيقاً مضطرداً دون تراجع ممن يقضى بها، لكى تقع موقع الرضا والتأييد من المجتمع الذى يترقب قضاءه[1].

واذا كان للنصوص القانونية الواردة فى قانون العقوبات خطورتها وأهميتها فإنه لا غناء لها عن القواعد الإجرائية، لأنها بدون هذه أما أن تفقد قوتها النافذة فتصير مجرد كلمات جوفاء وسطور صماء، واما أن يضطرد تطبيقها اذا تركت للقائمين على هذا التطبيق حرية أختيار مناهجها وطرقها، فيذهبون بذلك مذاهب شتا لا يكون فيها واحد تجاه الكافة، ولا يخلو من الشطط والانحراف من معاملة الناس، كما تتاح بها للقاضى على القانون سيادة، بدلاً من أن تكون السيادة عليه للقانون.

والقاعدة الإجرائية ليست غاية فى ذاتها، وانما هى وسيلة لغاية تتمثل فى

---

(١) د/ رءوف عبيد – مبادئ الإجراءات الجنائية (فى القانون المصرى) – دار الفكر العربى – القاهر – سنة ١٩٨٢ – ص ٥٠.

إحكام وحسن تطبيق القانون الجنائى الموضوعى، حتى قيل بحق أنها الأساس لدعوى تقام على الدعوى، أو لمحاكمة تخضع لها من جانب القانون المحاكمة الجارية على يد القاضى، فبينما تجرى بالدعوى العمومية محاكمة القاضى للمتهم، فإنه بتطبق القواعد الإجرائية التى خالفتها الدعوى تجرى محاكمة القانون للقاضى(١).

وتأسيساً على ما سبق فإن للإجراءات الجنائية خطورة لا تقل بحال عن القواعد المقررة فى القانون الموضوعى (العقوبات)، لأنها تمس مباشرة حريات المواطنين واستقرارهم بل إن قواعد العقاب تصبح لغواً وأداة محاباة فى يد الحاكم إذا لم تكن وليدة تدبير عميق عند وصفها، بما تستلزمه من حبس وإفراج، أو قبض وتفتيش، ومن قواعد للمحاكمة تطلب للخصوم ضمانات كافية لحيدة القاضى وسداد قضاءه، وأخرى للطعن فى الأحكام عندما تخطئ، أو تنفيذها عندما تصبح قرينة على الصواب(٢).

وأنطلاقاً من الدور الذى يؤديه قانون الإجراءات الجنائية، فإنه يمكن تعريفه بأنه القانون الذى ينظم وسائل التحقق من وقوع الجريمة ومحاكمة مرتكبيها،

---

(١) د/ رمسيس بهنام – الإجراءات الجنائية (تأصيلاً وتحليلاً) – منشأة المعارف – الإسكندرية – سنة ١٩٨٤ – ص ٦.

– وقد أضاف فى مرجعه القيم مقولة – يمثل قانون الإجراءات الجنائية النسق الشكلى من القانون الجنائى، بينما يعتبر قانون العقوبات بمثابة شقه الموضوع. نقلاً عن:

- R. Garraud: "Traité théorique et Pratique d'instruction criminelle et de Procédure Pénale". Paris. 1929, t.I. p. 3.

وقاعدة قانون الاجراءات الجنائية بوصفها قاعدة شكلية، فانها تملى قيداً يرد على سلوك رجال السلطة العامة ورجال القضاء، فيما يتعلق بأسلوب الكشف عن الجريمة الماثلة فى اهدار القاعدة الجنائية الموضوعية، وتعقب الجانى الذى اقترفها، والمطالبة بمحاكمته واجراء هذه المحاكمة واصدار الحكم فيها، وتنفيذ هذا الحكم.

- G. Vidal et J. Magnol., "Cours de droit criminel et de Science pénitentiaire", T.II Procédure Pénale. Paris, 1949 - p. 881

(٢) د/ رءوف عبيد – المرجع السابق – ص ٦.

وتوقع الجزاء عليهم، وينظم المحاكم الجنائية، ويحدد درجاتها واختصاصها، ويبين الاجراءات التى تتبع فى تحقيق الجرائم ومحاكمة مرتكبيها وتوقع العقوبات عليهم، وينظم سير الدعوى المدنية التى ترفع أمام القاضى الجنائى. واخيراً فإنه يضع القواعد الخاصة بالطعن على الاحكام الجنائية، ويكفل دقه وسلامة هذه الأحكام.

وتنحصر النظم الإجرائية التى تسود التشريعات فى مختلف الدول، وعلى مر العصور فى ثلاثة أنواع، وهى:

- النظام ا لاتهامى.
- نظام التنقيب والتحرى.
- ثم النظام المختلط.

ويندرج قانون الإجراءات الجنائية المصرى تحت النظام المختلط، حيث يجمع كغيره من النظم المعاصرة بين خصائص النظام الاتهامى، ونظام التفتيش والتحرى، فيغلب عليه طابع التنقيب والتحرى فى المرحلة التى تسبق رفع الدعوى إلى القضاء، فالدعوى الجنائية كقاعدة لا تطرح على القضاء مباشرة، بل تمر قبل ذلك بمرحلة التحقيق الإبتدائى وفيها تتم الإجراءات فى غير علانية، فلا يحضرها الجمهور ويصح أن يتخذ بعضها سراً فى غيبة الخصوم أنفسهم، ولذلك فإنه يلزم تدوين جميع الاجراءات فى هذه المرحلة، أما الأدلة فيتولى جمعها وتمحيصها موظفون عموميون، يجمعون فى إيدهم بين سلطة الاتهام وسلطة التحقيق. أما مرحلة المحاكمة فيغلب عليها الطابع الاتهامى، فإجراءاتها بحسب الأصل شفهيه وتجرى علناً بالنسبة للجمهور، وهى حضورية بالنسبة للخصوم، وقد يتقرر استثناء جعل المحاكم سرية لأسباب تتعلق بالنظام العام والآداب، وفى هذه الحالة تكون المحاكم سرية بالنسبة للجمهور وحده، أما الخصوم فلا يحال بينهم وبين حضورها على الأطلاق، ومن مظاهر النظام

الاتهامى فى هذه المرحلة إيجازت رفع الدعوى الجنائية مباشرة من المدعى بالحقوق المدنية، وتمكينه من تقديم أدلة الاتهام ضد المتهم(١).

على أن ذلك لا يعنى أن نظام التحقيق تنقيبى خالص، ولا أن نظام المحاكمة أتهامى صرفاً، ففى كل مرحلة تجتمع وتختلط خصائص التنقيب والاتهام، وأنما يمكن القول بسيادة الطابع التنقيبى فى مرحلة التحقيق، وغلبة الطابع الاتهام فى مرحلة المحاكمة(٢).

**ثانياً: الشرعية الإجرائية لجرائم المعلوماتية:**

**- سيادة القانون والشرعية الدستورية:**

يسود المجتمع الدولى المعاصر مبدأ سيادة القانون رغم اختلاف بعض الدول فى تحديد مضمونه. ومقتضى هذا المبدأ التزام جميع أعضاء المجتمع وأجهزة الدولة بالقوانين التى تصدرها السلطة المختصة(٣) كأساس لمشروعية أعمال هذه السلطة. ولا شك أن هذا المبدأ يضمن احترام حقوق الأفراد وحرياتهم فى مواجهة السلطة العامة، لأنها تصبح محكومة بالقانون وحده بعيداً عن أهواء السلطة أو تحكمها. وبهذا يحقق مبدأ سيادة القانون الأمن للأفراد عن طريق التزامهم بالقوانين التى تسرى عليهم والتزام سلطات الدولة باحترامها وتطبيقها. وقد اصطلح على تسمية المبدأ فى انجلترا بأسم "Principal of Rule of Law" أى مبدأ «حكم القانون»، كما يطلق عليه فى الولايات المتحدة الأمريكية أسم "The principal of limited government" أى مبدأ «الحكومة المقيدة»، وأحياناً يطلق عليه تعبير «حكومة قانون لا حكومة أشخاص» "A goverogment of laws not of men". كما يطلق عليه فى مصر وفرنسا «مبدأ سيادة القانون» "Prééminence du droit".

---

(١) د/ عوض محمد عوض – المبادئ العامة فى قانون الإجراءات الجنائية – دار المطبوعات الجامعية – الإسكندرية – سنة ١٩٩٩ – ص ١٦.

(٢) المرجع السابق، ص ١٦.

(٣) أنظر/ طعيمة الجرف –مبدأ المشروعية، ص ٣ وما بعدها.

وقد عني الدستور المصري بالنص على أن سيادة القانون أساس الحكم في الدولة (المادة ٦٤)(١).

وقد عبرت المحكمة الدستورية العليا في مصر عن مبدأ سيادة القانون قائلة بأن (الدولة القانونية هي التي تتقيد في كافة مظاهر نشاطها - وأيا كانت طبيعة سلطاتها - بقواعد قانونية تعلو عليها، وتكون بذاتها ضابطاً لأعمالها وتصرفاتها في أشكالها المختلفة، ذلك أن ممارسة السلطة لم تعد إمتيازاً شخصياً لأحد، ولكنها تباشر نيابة عن الجماعة ولصالحها)(٢).

• **الشرعية المعنية:**

ويلاحظ أن تطبيق هذا المبدأ بطريقة مجردة لا يؤمن المواطنين إلا بضمان معرفتهم بالقانون الواجب التطبيق، وبضمان تطبيقه عليهم وعلى جميع أجهزة الدولة على قدم المساواة.

ولكن ماذا يكون الحل لو كان القانون غير عادل أو غير إنساني؟ إن هذا الأمن والضمان لن يكون في هذه الحالة غير مجرد عزاء تافه لضحايا القانون(٣). وفي هذه الحالة يصبح مبدأ سيادة القانون عديم الفاعلية إذا لم يحقق أدنى أمن حقيقي لأعضاء المجتمع، أو لم يكفل أي قيد على سلطة أجهزة الدولة، إذا كان قد أباح لهذه الأجهزة سلطات واسعة بغير حدود. وإذن فلابد من وجود صمام أمن يكفل إعطاء المضمون الفعال لمبدأ سيادة القانون ويضمن تحقيق

---

(١) د/ أحمد فتحي سرور - الشرعية الدستورية وحقوق الإنسان في الاجراءات الجنائية - دار النهضة العربية - سنة ١٩٩٣ - ص ١٢٩.

(٢) المحكمة الدستورية العليا في ٢٣ يناير سنة ١٩٩٢ - في القضية رقم ٢٢ لسنة ٨ قضائية «دستورية» - الجريدة الرسمية - العدد ٤ - في ٢٣ يناير سنة ١٩٩٢.

(3) NORMANS. MARSH: Commission internationale de juristes, le principe de la légalité dans une société libre, (Rap - port sur les travaux du congrés international des jurtistes tenu à New Delhi, Janvier 1959, p. 62).

أهدافه، وهو مبدأ الشرعية (المعنى الدقيق) . والشرعية التى تعنيها هى تلك المبادئ العامة التى نتقيد بها . وفى النظام الديمقراطى يجب أن تكفل هذه المبادئ احترام حقوق الانسان واقامة التوازن بينها وبين المصلحة العامة(١) .

ومن هنا يتضح أن الشرعية الدستورية وسيادة القانون وجهان لعملة واحدة، فالشرعية الدستورية هى المبدأ، وسيادة القانون هى التزام سلطات الدولة باحترام هذا المبدأ ومطابقة أفعالها معه . ويلاحظ أن هذه المطابقة تسمى أحياناً بالمشروعية (Légitimité) تمييزاً لها عن الشرعية (Légalité) .

ويتجلى التزام السلطة التشريعية بسيادة القانون من خلال التقيد بالشرعية الدستورية فيما توافق عليه من قوانين(٢) .

أ - مشروعية الإجراء القانوني:

وفى نطاق بسط النظم العقابية على كافة الأفعال المرتكبة مخالفة للقانون . فإنه يتعين على المشرع الوطنى سرعة التدخل بسن تشريعات وحصر نماذج الإجرام المعلوماتي والنص على قواعد وأسس العقاب عليها، وكذلك تنظيم الاجراءات الجنائية المتبعة حال الاستدلالات والتحقيق الجنائي والمحاكمة . وفى هذا الشأن لا تثريب على المشرع أن هو تحلل فى هذه الاجراءات من القيود التقليدية المعروفة فى التشريعات الجنائية الإجرائية، شريطة عدم الاخلال بالمشروعية الموضوعية أو الإجرائية، وأيضاً عدم الاخلال بحقوق المواطن الدستورية . ذلك لأن ا لجريمة المعلوماتية هى جريمة غير تقليدية، هى جريمة

---

(١) د/ أحمد فتحى سرور – المرجع السابق – ص ١٣٠ .

(٢) للمزيد من التفصيل بشأن مبدأ الشرعية الجنائية أنظر بوجه خاص:

- BENL ATRCHE (A bd elouahab): "Le principle de la pegatite criminelle. Etude de droit compare" these poitiers 1981.

وأيضاً يراجع: د/ هلالى عبد اللاه أحمد – شرح قانون العقوبات (القسم العام) – دار النهضة العربية – القاهرة – ط ١ – سنة ١٩٨٧ – ص ٤٦٤ وما بعدها.

العصر المعلوماتى (الحادى والعشرين)، لا يُرى الجانى فيها، ولا يُرى فعله بوصف أنه لا يخلف آثاراً مادية - ملموسة - خلفه، ومن ثم فإن اجراءات ضبطه وضبط دليل الإثبات لفعله - وهو دليل علمى فى المقام الأول - يجب أن يتحرر من الصيغ التقليدية وينطلق ليوائم التقنية العلمية، شريطة عدم المساس بالحقوق الدستورية وبمبدأ المشروعية[1].

• ماهية المشروعية:

تُعرف المشروعية بأنها:

«التوافق والتقيد بأحكام القانون فى إطاره ومضمونه العام، لذلك فهى تهدف إلى تقرير ضمانة أساسية وجدية للأفراد لحماية حرياتهم وحقوقهم الشخصية ضد تعسف السلطة، وبالتطاول عليها فى غير الحالات التى رخص فيها القانون بذلك، من أجل حماية النظام الاجتماعى، وبنفس القدر تحقيق حماية مماثلة للفرد ذاته»[2].

(١) يراجع بشأن: Le principe de la legalité de la Preuve penale
مبدأ شرعية الإثبات الجنائى: د/ محمد ذكى أبو عامر - الإثبات فى المواد الجنائية - الفنية للطباعة والنشر - الإسكندرية - بدون سنة نشر - ص ١١٦ وما بعدها.
- فشرعية الإثبات الجنائى تستلزم عدم قبول أى دليل يكون البحث عنه أو الحصول عليه قد تم بطريق غير مشروع، فهذا البحث مقيد باحترام (حقوق الدفاع) من جهة، (وقيم العدالة وأخلاقياتها) من جهة أخرى، (ومقتضيات الحفاظ على كرامة الإنسان) من جهة أخيرة، وهو ما لا يتأتى إلا اذا كان البحث عن الدليل قد تم باستخدام اجراءات مشروعة Moyèns legaux.
ويراجع أيضا فى ذات المؤلف بخصوص: القيمة الاثباتية للأدلة العلمية ومدى اعتبارها دليلاً مستقلاً أم مجرد قرائن - المرجع السابق - ص ١٢١ وما بعدها.
ويعلق جانب من الفقة على القصور التشريعى فى مجال الجريمة المعلوماتية وما تستهدفه فى نطاق التجارة الإليكترونية بقوله: (إن التجارة الإليكترونية تبحث عن قانون). راجع:
- Michel vivant, commerçe élétronique cherche droit, droit et patrimoine, No, 55, Décembre 1991, p. 50.

(٢) د/ أحمد ضياء الدين - مشروعية الدليل فى المواد الجنائية - بدون ناشر - سنة ١٩٨٣ - ص١٠٢.

- لذلك فمن الأهمية لصحة الإجراءات التى يمارسها مأمور الضبط القضائى، أن تغلف بمبدأ المشروعية، مما يثمر عن دليل صحيح يعول عليه القاضى فى أحكامه، لأن الإجراءات القانونية اذا كانت باطلة وأثمرت عن دليل صحيح، فإن القاضى لا يلتفت إليه. لأن الهدف الذى يسعى إليه القانون هو حماية حقوق وحريات أفراد المجتمع من عسف السلطة (ممثلة فى منفذوا القانون)، وما حاجة العدالة إلى دليل صحيح فى الإدانة باطل فى الأساس فما بنى على باطل يكون باطلاً. وخيراً للعدالة أن يبدأ الجانى إذا كان دليل ادانته سنده غير مشروع واهن فى أساسه، باطل فى إجراءه.

لذلك فقد أوكل القانون للجهات القضائية، رقابة مشروعية اجراءات الاستدلال والتفتيش والضبط(1)، فى الأحوال التى يجوز فيها لمأمورى الضبط القيام بها، ومن هذه القواعد العامة يتم التطبيق فى مجال ضبط الجريمة المعلوماتية، وكذلك فى التأكد من قانونية ضبط الدليل المعلوماتى المتحصل من هذه الإجراءات.

كما يقصد بمبدأ المشروعية ضرورة احترام القواعد القانونية القائمة. بأن تكون كل تصرفات السلطات العامة والأفراد فى إطار القانون، وهذا يعتبر فى الدولة المعاصرة حداً أعلى لسلطان الحاكم وتصرفات الهيئات العامة والمحكومين، ويتطلب الالتزام بالقانون الطبيعى وما يختزنه من مبادئ قانونية عامة يحتويها ضمير الجماعة، ويستقر عليها باعتبارها ركائز أساسية لمعنى العدل والصالح العام. كما يتطلب أيضاً الالتزام بالمشروعية الوصفية التى تستقر

---

(1) د/ أحمد فتحى سرور – الوسيط فى قانون الإجراءات الجنائية – دار النهضة العربية – ط ٧ – سنة ١٩٩٧ – ص ١٠٤.

* بالنظر إلى كشف الحقيقة، لا تخضع النيابة العامة فى تصرفاتها لغير مقتضيات الحقيقة، وعليها أن تتأكد قانوناً من مسئولية المتهم. ومن واجبها أيضاً حماية مصالح المتهم عند الاقتضاء. فهى تتعاون مع القاضى فى كشف الحقيقة والبحث عن المتهم الحقيقى، لا وضع أى شخص موضع الأتهام.

على مبدأ سيادة الدستور والتشريع، وما يفرضه ذلك من ضرورة الالتزام بقاعدة القانون الأعلى أياً كان مصدرها[١].

وخلال الفترة التى اختلطت فيها السلطة والسيادة بشخصية الحاكم، لم يكن مبدأ المشروعية شيئاً يذكر، فلا حقوق ولا حريات سوى تلك التى تتمتع بها السلطة الحاكمة، وتلك المتاحة لمنفذ سياسة هذه السلطة، وقد كان ذلك فى العصور القديمة والوسطى، بل وفى بعضاً من الدول النامية الفقيرة فى العصر الحديث.

ولم يكن هذا الوضع ليستمر أمام التيار الديمقراطى الجارف، وأمام النظريات السياسية التى أرجعت السلطة للشعب، وبدأت تظهر فى الآفاق الدولة القانونية، التى يقصد بها التزام الأفراد والسلطات المسئولة بالقانون وأحكامه[٢].

**ب -المشروعية في مرحلة جمع الاستدلالات:**

لقد أقر المشرع فى قانون الإجراءات الجنائية اختصاصات معينة لمأمورى الضبط القضائى عند البدء فى أعمال التحقيق، وذلك لحرصه على سرعة ضبط الواقعة وعدم طمس الأدلة التى تدل على الفاعل وبالتالى ضياع معالم الجريمة. وصعوبة أقرار العدالة بشأنها، وما يقتضيه ذلك من سرعة انتقال مأمور الضبطية القضائية لمكان ارتكاب الجريمة، ومباشرة ما خوله له المشرع من اختصاصات.

---

(١) د/ السيد خليل هيكل – موقف الفقه الدستورى التقليدى والفقه الإسلامى من بناء وتنظيم الدولة – دار النهضة العربية – القاهرة – سنة ١٩٨٩ – ص ١٦٦، د/ محمد أنس جعفر الوسيط فى القانون العام – دار النهضة العربية – ط ٢ – سنة ١٩٩٠ – ص ١٢.

(2) Voir aussi en ce sens:

- De laubadére (André): Traité élémentaire de droit admini Stratif - T.1,7eme éd., L.G.d.J., Paris, 1976, 1976, p. 193.

Zissiadis: La Rôle des oarganes de poursuite dans le Pénal en droit Hellinque, Rev. Inter. Drioit Pénal, 1963, p. 181.

ويشترط فى تلك الاختصاصات عدم المساس بحرمة شخص المتهم أو مسكنه وعدم أهدار حقوقه، وذلك ما يميز هذه الاختصاصات عن إجراءات التحقيق بمعناها الضيق، والتى لا تكون إلا بعد ظهور الجريمة، ويتجه فيها التحقيق إلى متهم معين دون غيره.

وتعتبر أهم اجراءات الاستدلال والتى أقرها مبدأ المشروعية، ما نصت عليه المادة ٢١ إجراءات جنائية:

«يقوم مأمور الضبط القضائى بالبحث عن الجرائم ومرتكبيها وجمع الاستدلالات التى تلزم للتحقيق فى الدعوى».

«يجب على مأمورى الضبط القضائى أن يقبلوا التبليغات والشكاوى التى ترد إليهم بشأن الجرائم، وأن يبعثوا بها فوراً إلى النيابة العامة ويجب عليهم وعلى مرءوسيهم أن يحصلوا على جميع الإيضاحات ويجروا المعاينات اللازمة لتسهيل تحقيق الوقائع التى تبلغ إليهم، أو التى يعلنون بها بأية كيفية كانت، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة».

«لمأمورى الضبط القضائى أثناء جمع الاستدلالات أن يسمعوا أقوال من يكون لديه معلومات عن الوقائع الجنائية ومرتكبها وأن يسألوا المتهم عن ذلك، ولهم أن يستعينوا بالأطباء وغيرهم من أهل الخبرة ويطلبوا رأيهم شفهياً أو بالكتابة.

ولا يجوز لهم تحليف الشهود أو الخبراء اليمين إلا إذا خيف ألا يُستطاع فيما بعد سماع الشهادة بيمين»(*).

---

(*) يراجع بشأن تنظيم المُشرع لمأمورى الضبط القضائى وواجباتهم: د/ طارق ابراهيم الدسوقى- مقالة بذات العنوان - مجلة الأمن العام - العدد ١٩٥ - السنة ٤٨ - أكتوبر ٢٠٠٦ - ص ٥٣ وما بعدها.

وعلى ذلك فإنه اذا تطلبت أعمال الاستدلال (لأحد جرائم المعلوماتية) تدخل مأمور الضبط القضائى فى حرمة الحياة الخاصة لشخص - مشتبه فيه - ما، إذا كانت المعلومات الواردة عن وقوع الجريمة تفيد أن محل الجريمة هو المعلومات الموجودة داخل حاسب آلى يخصه (بالملكية أو اداء العمل أو التأجير لوقت)، فإن مضمون مبدأ المشروعية لا يجيز لمأمور الضبط القضائى مغبة اختراق الحياة الخاصة لهذا الشخص، أو اتخاذ أى إجراءات من شأنها انتهاك حرمة حياته الخاصة (سواء بالدخول إلى مسكنه أو بالمساس بشخصة)(*)، ولكن حق المجتمع فى الحماية يقتضى سرعة اتخاذ ما نص عليه القانون من إجراءات قانونية لضبط الواقعة ومرتكبها. (المادة ٣٤، ٣٥ إجراءات جنائية)، بالإضافة إلى إعمال مأمور الضبط القضائى لنصوص المواد (٣٠، ٣١، ٣٢، ٣٣ إجراءات جنائية)، فى حالة كون الجريمة المعلوماتية متلبساً بها.

**جـ- المشروعية والدلائل الكافية:**

يثير تطبيق مأمور الضبط القضائى لنص المادة ٣٤ من قانون الإجراءات الجنائية(**) فى نطاق الجرائم المعلوماتية مشكلة فى تفسير الدلائل الكافية على الاتهام، ومدى تطابق ذلك مع احترام مبدأ المشروعية الإجرائية.

---

(*) لذلك فإن قيام مأمورى الضبط القضائى فى سبيل جمع الاستدلالات، بالدخول إلى أنظمة معلوماتية - حاسبات آلية، انترنت - لأشخاص المتهمين - مشتبه فيهم - لا شك أن هذا الإجراء يكون خارجاً عن حدود المشروعية، مما يترتب عليه بطلان ما تم اتخاذه من إجراءات.

(**) تنص المادة ٣٤ إ -جـ على أنه:

«لمأمور الضبط القضائى فى أحوال التلبس بالجنايات أو الجنح التى يعاقب عليها بالحبس لمدة تزيد على ثلاثة أشهر، أن يأمر بالقبض على المتهم الحاضر الذى توجد دلائل كافية على اتهامه».

(معدلة بالقانون رقم ٣٧ لسنة ١٩٧٢ - الجريدة الرسمية العدد ٣٩ الصادر فى ١٩٧٢/٩/٢٨).

**تأصيل المسألة وتفسيرها:**

أختلف تحديد مدلول الدلائل الكافية Indices suffisantes فى القضاء المقارن ما بين تعريفها على أساس كونها شبهات مستمدة من الواقع والقرائن، أو إنها أقل من هذا التحديد، باعتبارها ذات وضعية جنائية مطلقة، من حيث أنها مظاهر خارجية تنبئ عن ارتكاب شخص لجريمة من الجرائم المحددة حصراً بها[1].

وسوف نعرض لهذه المسألة، فى النظام الإجرائى الفرنسى والمصرى والأمريكى.

**أ - الوضع في النظام الإجرائي الفرنسي:**

استخدم المشرع الفرنسى فى قانون الإجراءات الجنائية تعبرات عديدة الدلالة على الدلائل الكافية، فقد استخدم عبارة Indices graves et concordants (دلائل خطيرة ومترابطة) فى المادتين ٦٣/٢، ١٠٥، واستخدم عبارة Des charges constitutives d'infraction فى المادة ١٧٦، وعبارة Des charges suffisantes (إثباتات كافية) فى المواد ١٧٧، ٢١١، ٢١٢. والناظر المتأمل فى هذه النصوص يجد إنها لم تورد تعريفاً دقيقاً لمعنى الدلائل الكافية[2].

ولا يختلف الأمر على الصعيد القضائى. فأحكام محكمة النقض لم تشأ أن تحدد معنى كفاية الدلائل، بل كل ما ذكرته فى أحكامها مجرد أمثلة لما لا يعد داخلاً فى مفهوم الدلائل الكافية[3].

---

(١) د/ رءوف عبيد – المشكلات العملية الهامة فى الاجراءات الجنائية – دار الفكرى العربى – القاهرة – جـ١ – ط ٣ – سنة ١٩٨٠ – ص ٣١.

(٢) د/ هلالى عبد اللاه أحمد – المركز القانونى للمتهم فى مرحلة التحقيق الإبتدائى (دراسة مقارنة) – دار النهضة العربية – ط ٢ – سنة ٢٠٠٤ – ص ٤٨.

(3) Cass. Crim. 22 Juillet, 1954, J. C.P. 1954, II, 8351, note r. Vouin.

ولذا حاول جانب من الفقه تعريف الدلائل الكافية بأنها عبارة عن: «أمارات معينة تستند إلى العقل وتبدأ من ظروف أو وقائع يستنتج منها الفعل، توحى للوهلة الأولى بأن جريمة ما قد وقعت، وان شخصاً معيناً هو مرتكبها»(١). بيد أن هذه الامارات لا يكفى فى تقديرها مجرد المنطق، بل لابد فى شأنها من الخبرة والتعقل(٢). وعموماً يمكن القول بأن الدلائل الكافية هى كل ما لا يدخل فى الأدلة الأخرى(٣).

**ب- الوضع في النظام الإجرائي المصري:**

استخدم قانون الإجراءات المصرى فى المواد ٣٤، ٣٥، ١٣٤ تعبير دلائل كافية. ثم استخدم تعبير الأدلة الكافية فى المادة ٢١٤. والنصوص التى ورد بها هذا التعبير لم يشأ أيا منها أن يضع تعريفاً لهذه الدلائل. فالهدف من ايراد تعبير الدلائل الكافية فى النصوص السابقة ليس تعريفها، وإنما ايجاد رخصة لمأمور الضبط القضائى أو المحقق باتخاذ اجراءات معينة عند توافرها(٤).

وبالنسبة لمحكمة النقض فهى وان كانت قد بينت المقصود بالدلائل الكافية فى حكمها الى نصت فيه على أن: «المقصود من كفاية الأدلة فى قضاء الإحالة إنها تسمح بتقديم المتهم للمحاكمة مع رجحان الحكم بإدانته»(٥). فإنها لم تحدد معنى الدلائل الكافية بوصفها شرطاً لاكتساب الشخص صفة المتهم. بل كل ما

---

(1) GORPHE (F.): "L'appreciation de preuves en justice, essai d'une methode technique" Sirey 1947, p. 247.

(2) MERLE (R.) et vitu (A.): "Traite de droit criminel" de. Y. Cujas, Tome II. "Procedure Penale" 3e - ed - 1979, no. 784, p. 757.

(3) GORPHE (F.): Op. Cit. p. 246.

(٤) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٤٩.

(٥) نقض ٢٥ أبريل ١٩٦٧–مجموعة أحكام النقض – س ٣٦ ق – رقم ١١٣ – ص ٥٦٩.

أوردته فى أحكامها مجرد أمثلة فتوافر الدلائل الكافية(١)، أو عدم توافرها(٢)، مع الإشارة إلى أن تقدير الدلائل ومبلغ كفايتها يكون بداءة لمأمور الضبط القضائى، على أن يكون تقديره هذا خاضعاً لرقابة سلطة التحقيق تحت أشراف محكمة الموضوع(٣).

وعلى مستوى الفقة(*) ذهب رأى إلى أنه يصعب وضع تعريف جامع مانع للدلائل الكافية(**)، إذ ليس هناك معادلة حسابية يمكن أن نقيس بها بدقة الظروف المختلفة التى قد تبنى عليها الدلائل الكافية للاتهام. وانما ينبغى أن نأخذ كل الظروف فى الاعتبار، ونزنها بميزان عادل حتى نحدد ما يعتبر من

(١) يراجع: نقض ١٩ ديسمبر ١٩٨١ – مجموعة أحكام النقض – س ٥١ ق – رقم ٢٠٥ – ص ١١٤٤. وفى هذا الحكم قضت محكمة النقض: «... وإذ كانت هذه الجريمة جنحة معاقباً عليها بالحبس الذى تزيد مدته على ثلاثة أشهر، وكانت قد توافرت لدى مأمور الضبط القضائى وفقاً لما تشير إليه ملابسات الواقعة وظروفها التى أثبتها الحكم، دلائل جدية كافية على اتهام المطعون ضده بارتكابها، فانه من ثم يكون له أن يأمر بالقبض عليه مادام أنه كان حراً وذلك عملاً بالمادة ٣٤ إ-ج المعدلة بالقانون رقم ٣٧ لسنة ١٩٧٢ المتعلق بضمان حريات المواطنين».

(٢) ولذا قضت بأن وجود شخص فى الطريق العام فى وقت متأخر من الليل، وتناقضه فى أقواله عند سؤاله عن أسمه وحرفته، لا ينبئ بذاته عن تلبس، ولا يوحى إلى رجل الضبط بقيام أمارات أو دلائل على ارتكابها حتى يسوغ له القبض عليه وتفتيشه. (نقض ١٩ يناير سنة ١٩٧٥ – مجموعة أحكام النقض – س ٨ ق – رقم ٢٨ – ص ٩٥).

(٣) نقض ٨ أكتوبر سنة ١٩٨٠ – مجموعة أحكام النقض – س ٥٠ ق – رقم ١٦٣ – ص ٨٤٣، نقض ١٠ نوفمبر ١٩٧٤ – أحكام النقض – س ٢٥ ق – رقم ١٥٥ – ص ٧١٥، نقض ١٣ نوفمبر ١٩٧٣، أحكام النقض – س ٢٤ ق – رقم ٢٠٣ – ص ٩٧٢.

(*) هناك تفرقه من حيث القوة بين الدلائل الكافية لكى يكتسب الشخص صفة المتهم والدلائل الكافية لإحالة المتهم إلى سلطات المحاكمة، إذ يكفى فى الأولى الشكوك المعقولة، أما فى الثانية فيشترط أن تكون من القوة بحيث ترجح الإدانة على البراءة. (د/ أحمد فتحى سرور – الوسيط فى الإجراءات الجنائية – مرجع سابق – بند رقم ٢٤٨ – ص ٦٦٦).

(**) هذا التعبير لا يختلف كثيراً عن عبارة دلائل خطيرة Endices graves التى كانت فى المادة ١٥ من قانون تحقيق الجنايات الملغى. (أ/ أحمد عثمان حمزاوى – موسوعة التعليقات على قانون الإجراءات الجنائية – دار النشر للجامعات – القاهرة – سنة ١٩٥٣ – ص ٢٤٥).

الدلائل وما لا يعتبر كذلك[1]. فيما ذهب رأى آخر إلى أن الدلائل هى[2]: «العلامات الخارجية أو الشبهات المقبولة دون ضرورة التعمق فى تمحيصها وتقليب وجوه الرأى فيها. وهى لا ترقى إلى مرتبة الأدلة. فهى قرائن ضعيفة، أى استنتاج لأمر مجهول من أمر معلوم، لكن ضعفها يجئ من استنتاجها من وقائع قد لا تؤدى إلى ثبوت التهمة بالضرورة الحتمية ولا بحكم اللزوم العقلى. فهى لا تصلح وحدها – أمام محكمة الموضوع – سبباً للإدانة بل للبراءة، عملاً بنص المادة ٣٠٤ إجراءات التى تنص على أنه إذا كانت الواقعة غير ثابتة أو كان القانون لا يعاقب عليها تحكم المحكمة ببراءة المتهم.

ويترتب على توافر الدلائل الكافية قبل الشخص المراد القبض عليه، أثران هامان[3]:

الأول: الأمر بالتحفظ على المتهم، وقد عبرت عن ذلك المادة ٣٥ إ–جـ حيث نصت على أن: «... جاز لمأمور الضبط القضائى أن يتخذ الإجراءات التحفظية المناسبة».

ويراد بذلك الإجراءات التى يكون من شأنها أن تحول دون فرار المتهم أو تأثيره عى أدلة الدعوى. وتتنوع الصور التى تتخذ فى هذا الشأن، فقد تأخذ شكل الاستيقاف أو الاقتياد إلى مقر الشرطة، أو الاحتجاز لفترة من الوقت أقل

(١) د/ سامى حسنى الحسينى – النظرية العامة للتفتيش فى القانون المصرى والمقارن – دار النهضة العربية – سنة ١٩٧٢ – ص ١٩٩.

(٢) د/ رؤوف عبيد – مرجع سابق – ص ٣١.
وراجع أمثلة للدلائل الكافية وردت فى قضاء محكمة النقض المصرية فى الأحكام التالية:
نقض ١٤ أكتوبر ١٩٦٨ – مجموعة أحكام النقض – س ١٩ ق – رقم ١٦٥ – ص ٨٣٥، نقض ١٢ ديسمبر ١٩٦٠ – مجموعة أحكام النقض – س ١١ ق – رقم ١٧٢ – ص ٨٨٣.

(٣) د/ هلالى عبد اللاه أحمد – ضمانات المتهم فى مواجهة القبض (بين الشريعة الإسلامية والقانون الوضعى) – دار النهضة العربية – سنة ٢٠٠٠ – ص ١٠٢.

من ٢٤ ساعة، وهو الحد الأقصى للقبض الذى يملكه مأمور الضبط القضائى. (المادة ٣٦ إ-جـ).

**الثاني:** استصدار أمر من النيابة بالقبض على المتهم.

فإذا لم تستجيب النيابة العامة إلى طلب القبض وجب إلغاء التحفظ.

**جـ- الوضع في النظام الإجرائي الأمريكي:**

عبر قانون الإجراءات الجنائية الأمريكى عن الدلائل الكافية باصطلاح السبب المعقول أو المحتمل. كما استخدم التعديل الرابع للدستور الأمريكى نفس هذا التعبير، حين نص على حق المواطنين فى تأمينهم فى أشخاصهم ومنازلهم وأرواحهم ومستنداتهم ضد أى قبض أو تفتيش غير قانونى، وعلى وجوب عدم إصدار أوامر قبض أو تفتيش ما لم تكن بناء على سبب معقول(١).

كذلك درج القضاء الأمريكى على استخدام هذا المصطلح فى أحكامه المختلفة(٢). ومن ذلك ما قضت به المحكمة العليا فى الولايات المتحدة الأمريكية أن السبب المعقول لا يعنى أكثر من الشك البسيط. واستطردت تقول أن السبب المعقول يوجد فى حالة الوقائع والظروف التى تكفى بذاتها للدلالة فى تقدير الشخص الحريص Pruden man – على وقوع جريمة من الشخص الذى يراد القبض عليه(*).

---

(1) CAREY (John): "Kles criteres minimum de la Justice criminelle aux Etats - unis" R.I.D.P. 1966, pp. 77 ets.

- MULLENGACH (Linda Herman): "Warrontless residential searches to prevent the destruction of evidence. A need for strict stendards" the Journal of criminal law, criminology, Volume 70 number 2, 1979, pp. 255, etgs.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٥٣ وما بعدها.

(*) حكمت المحكمة العليا لولاية اهايو Ohio بأن السبب المعقول يتوفر عندما تكون الأفعال والظروف تنبئ فى تقدير ذوى الفطنة، أن الشخص المشتبه فيه قد ارتكب جريمة أو أنه فى

=/=

كما أتجه القضاء الأمريكى إلى التمييز بين الدلائل الكافية فى معنى السبب الكافى أو الشبهات المعقولة(*). وبين السبب المحتمل Probable cause الذى يبنى على الاحتمال Probability تحديداً، إلا أن هذا الأخير لا يحتاج إلى أن يكون مساوياً فى الدرجة أو معتمداً على سبب كاف أو شبهة معقولة أو قوية، فالاساس فى السبب المحتمل إنه مبنياً على الاحتمال، لذلك هو أقرب إلى الدلائل الكافية. لذلك فإن منطق السبب الكافى يعد أقوى مرحلياً فى الإجراءات الجنائية، بحيث لا تحتاج إلى تبرير بلزوم توافر دليل ما، أو امكانية كبيرة لتوافره، لكى يقوم

---

— مجرى تنفيذه لها. يستوى فى ذلك أن يكون علم مأمور الضبط القضائى بالجريمة قد تم بواسطته شخصياً، أم عن طريق بلاغ مقدم من الغير.

وأيضا يراجع: - Bringar V. United states, 338 U.S. 160, 175, 75, 1946.

- حكم المحكمة العليا فى ولاية تكساس، أن مجرد رفض الشخص المشتبه فيه الافصاح عن شخصيته لا يكون السبب المعقول Probable cause.

- Brown V. Texas 443 U.S. 47, 1979.

- وأيضاً حكمت المحكمة العليا فى ولاية كاليفورنيا California أن إحجام المشتبه فيه عن طلب براءته وقت إلقاء القبض عليه لا يكفى لتوافر السبب المعقول.

- Chimel V. California, 395 U.S. 752, 1969.

- وحكم بأن السبب المعقول لا ينشأ من مجرد تواجد شخص صحبة مجموعة أفراد، كان يشتبه فى ارتكابهم أعمالاً إجرامية.

- United states V. Dire, 332 U.S. 581, 1948.

(*) يكتفى القضاء الامريكى بوجود اختراق لقاعدة تنظيمية – كما هو الشأن فى قانون الاجراءات الجنائية لولاية نيويورك الذى يعتبر ارتكاب الشخص لجرائم صغيرة Petty offences – مثل عدم التزام قائد دراجة بقواعد المرور على الطرقات من الدلائل الكافية فى معنى السبب الكافى أو الشبهة المعقولة Probable cause (Reasonable-Suspicion) التى تسمح باطلاق السلطات الاستثنائية لمأمور الضبط القضائى من السؤال عن الهوية والتفتيش والقبض... الخ. وقد حكمت المحكمة العليا فى ولاية ميسيسبى Mississipi أن قول المجنى عليه فى جريمة سرقة بأن الذى اعتدى عليه وأخذ ماله هو شاب ذو بشرة سوداء لا يكون سبباً معقولاً يبرر القبض على شخص له نفس هذه الأوصاف. يراجع:

- KEBEICH (Mahmoud): "L'inculpation et ude du droit francais, essai de rapprochement avec le droit egyptien et le droit des Etats-unis d'Amerique" These pour le doctorate d'Etat, Poitiers 1984.P. 202.

مأمور الضبط القضائى باجراء التفتيش مثلاً. بل يكفى أن يقرر مأمور الضبط القضائى أن تفتيش الحاسب الآلى فى منزل أحد الأشخاص سوف يؤدى إلى وجود أدلة تدينه، وذلك لوجود مؤشرات خارجية على وجود هذه الأدلة بحوزة الشخص المشار إليه(١).

والواقع أن منطق التعامل مع الدلائل الكافية فى جرائم المعلوماتية يمكن أن يكون مصدراً للخطورة والتهديد للحريات. فالأمر أكثر من مجرد تفهم موقف معين على أنه يشكل جريمة فى القانون، لذلك لا يمكن السماح بما هو مقرر فى القانون من سلطات لمأمور الضبط القضائى، لمجرد أن توافرت دلائل كافية على ارتكاب شخص ما لجريمة، وإنما تسمح الدلائل الكافية فى نظام معلوماتى – فى حاسب آلى، أو عبر الأنترنت – بلغت انتباه مأمور الضبط على أن جريمة وقعت وأنه قد تم التعرف على مرتكبها(٢).

ومثل هذا الأمر يجعلنا نأخذ فى الاعتبار عدم إمكانية وضع قاعدة عامة للدلائل الكافية فى نظم المعلوماتية، كما هو الحال فى الجرائم التقليدية، فليس لمأمور الضبط القضائى أن ينفذ إجراء القبض على شخص ما لمجرد توافر دلائل كافية على ارتكابه جريمة من جرائم المعلوماتية، وان كان من الممكن أن يقوم باتخاذ الاجراءات التحفظية عليه (مادة ٣٥ إجراءات جنائية)، والفارق بين الإجرائين واضح المعالم، ففى حالة القبض فإن صلاحية استثنائية تتاح لمأمور الضبط القضائى، فى حين أن التحفظ على الشخص لا يعدو أن يكون تحفظاً وقتيا يرتبط باستكمال مأمور الضبط للإ جراء وهو أن يطلب من النيابة العامة أن تصدر أمراً بالقبض عليه.

(١) عمر محمد أبو بكر بن يونس – الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية) – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس – سنة ٢٠٠٤ – ص ٨٤٤.

(٢) المرجع ذاته.

وبناء على ذلك ليس لمأمور الضبط القضائى حال قيامه بمداهمة كافيه نت Caber Cafe القبض على شخص ما فيها - حتى ولو كان الشخص الوحيد الموجود ساعة المداهمة - لمجرد أن بلاغاً وصل إلى جهات الضبط القضائى، يفيد أن جريمة وقعت حالاً مصدرها هذا المكان ما لم يكن المبلغ حاضراً. لأن هذا الأخير (المبلغ) يعد شاهد عيان Eyewitness فى هذه الحالة، وبالتالى يعد ذلك سبباً كافياً Probable cause للقيام باتخاذ إجراء جنائى لأن السبب الكافى من الدلائل الكافية. أما اذا كان البلاغ من مجهول، أو كان بادياً من المبلغ حال تواجده أنه غير صادق، بحيث لم يستطع تأكيد ما أدعى بوجوده من وقائع إجرامية حال الواقعة، فإنه يجوز لمأمور الضبط - فقط - إعمال نص المادة ٢٤ إ-جـ من اتخاذ كافة الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة، ونص المادة ٣٢ إ-جـ التى تجيز له منع الحاضرين من مبارحة محل الواقعة، لحين قيام الخبراء - من رجال الأدلة الجنائية والمعلوماتية - بتقصى الحقائق ومعرفة تفصيلات الواقعة وضبط المخالفة القانونية المرتكبة.

## الفصل الأول

# الحماية الإجرائية القانونية للمعلوماتيــة

- المبحث الأول: إجراءات مواجهة الجريمة المعلوماتية.

  الفرع الأول: إجراء تفتيش نظم المعلوماتية.

  الفرع الثاني: ضبط نظم المعلوماتية.

- المبحث الثاني: الحماية الإجرائية للمعلوماتية في ضوء الاتفاقيات الدولية.

  الفـرع الأول: الإهتمام الدولي بالجوانب الإجرائية للجريمة المعلوماتية.

  الفرع الثاني: المشكلات العملية بشأن الحماية الإجرائية للمعلوماتية في ضوء اتفاقية بودايست ٢٠٠١.

# المبحث الأول

# إجراءات مواجهة الجريمة المعلوماتية

## الفرع الأول

## إجراء تفتيش نظم المعلوماتية

**البند الأول: القواعد العامة في إجراء التفتيش:**

التفتيش إجراء من إجراءات التحقيق يستهدف البحث عن الحقيقة فى مستودع السر، لذلك فهو يعتبر من أهم إجراءات التحقيق فى كشف الحقيقة لأنه غالباً ما يسفر عن أدلة مادية تؤيد إلى نسبة الجريمة إلى المتهم. وحينما يباشر ضابط الشرطة التفتيش بوصفه أحد مأمورى الضبطية القضائية، فهو يباشره إما على شخص المتهم وإما على مسكنه. فمحل التفتيش بالنسبة له لا يخرج عادة عن إحدى هذين الوعاءين.

هذا وقد تناول المشرع الإجرائى المصرى حق التفتيش فى الفصل الرابع من الباب الثانى من قانون الإجراءات الجنائية، حيث نص فى المادة ٤٦/ ١ على أنه:

«فى الأحوال التى يجوز فيها القبض قانوناً على المتهم يجوز لمأمور الضبط القضائى أن يفتشه».

وقد ورد فى المذكرة الإيضاحية عن هذه المادة ما يلى:

«وقد أقرت المادة ٨٣ المبدأ الذى صارت عليه محكمة النقض باستمرار، وهو تخويل مأمورى الضبط القضائى حق تفتيش المتهم فى الأحوال التى يجوز فيها قانوناً القبض عليه»(١) .

(١) الأستاذ/ أحمد عثمان حمزاوى - مرجع سابق - ص ٢٨٢.

* حيث يقابل المادة ٤٦ إ - جـ فى مشروع الحكومة المادة ٨٣.

وفى نطاق تفتيش المتهم المعلوماتى فإن هذا الإجراء يحصل بمعرفة مأمور الضبط القضائى،

-/-

ويعهد القانون إلى مأمور الضبطية القضائية بتفتيش شخص المتهم متى كانت الجريمة فى حالة تلبس، وإذا كانت أهمية إجراء التفتيش تكمن فى أنه يعد من أكثر الإجراءات فائدة فى إظهار الحقيقة، فإن ذلك يقتضى أن يباشره ضابط الشرطة بسمات معينة وقدرات متميزة، تمكنه من القيام بأداء هذا الإجراء بالشكل السليم الذى نص عليه القانون. وبالصورة التى تعكس اهتمام المنظمات الدولية بحقوق الإنسان فى إطار إعلانات حقوق الإنسان.

ويتحدد الإطار القانونى لحق التفتيش بإيضاح ماهية التفتيش، ثم بيان خصائصه التى تعد أيضاً شروطه الموضوعية التى يجب توافرها، ثم عرض الطبيعة القانونية للتفتيش، وكذلك استعراض الصور المختلفة التى يتخذها التفتيش من خلال النقاط الآتية:

أولاً: ماهية التفتيش La Perqusition.

ثانياً: خصائص التفتيش.

ثالثاً: الطبيعة القانونية لإجراء التفتيش.

رابعاً: صور التفتيش.

**أولاً: ماهية التفتيش La Perqusition:**

- **التفتيش عن الشئ لغة:** هو البحث عن مظان وجوده.
- **واصطلاحاً:** هو البحث عن الشئ فى مستودع السر.
- **وفقهاً:** تعددت التعريفات التى أضفاها الفقه على فكرة التفتيش(1)، إلا

---

-- فلا يجوز أن يعهد بذلك إلى أحد أعوانه، إلا إذا كان ذلك تحت بصره وإشرافه، كما أن طريقة التفتيش متروكة لتقدير القائم بها.

(1) راجع عن التفتيش باللغة العربية بالإضافة إلى الكتب العامة ما يلى:

* د/ السيد محمد سعيد عتيق – النظرية العامة للدليل العلمى فى الإثبات الجنائى – رسالة دكتوراة – كلية الحقوق – جامعة عين شمس – سنة ١٩٩٣م، د/ حسن صادق المرصفاوى – المحقق الجنائى – منشأة المعارف – الإسكندرية – بدون سنة نشر، د/ حسن شلبى يوسف – الضمانات -/-

-- الدستورية للحرية الشخصية فى التفتيش - رسالة دكتوراة - كلية الحقوق - جامعة القاهرة - سنة ١٩٩٢م، د/ حامد عبد الحكيم راشد - الحماية الجنائية فى حرمة المسكن - رسالة دكتوراة - كلية الحقوق - جامعة القاهرة - سنة ١٩٨٧م، أحكام تفتيش المسكن فى التشريعات الإجرائية العربية (دراسة مقارنة) - دار النهضة العربية - ط ١ - سنة ١٩٩٨م، د/ سامى حسنى الحسينى - النظرية العامة للتفتيش فى القانون المصرى والمقارن - رسالة دكتوراة - كلية الحقوق - جامعة عين شمس - سنة ١٩٧٠، د/ محمود محمود مصطفى - الإثبات فى المواد الجنائية فى القانون المقارن - الجزء الثانى (التفتيش والضبط) - مطبعة جامعة القاهرة - ط ١ - سنة ١٩٧٨.

* وراجع باللغة الإنجليزية:

- BUTTER (Publishers): "The search for evidence - London, 1985.
- RESING (D): "Searches and seizures" hand book - New Yourk, 1968.
- BAKER (E.R.) and DODGE (F.B): "Criminal evidence and procedure" London, Butter worhs, 6 tn 1987.
- ALLAN (H. Stoke): "Legal aspects of evidence" New York, 1985.
- ROADY (T.G.) and others: "Essays on procedure and evidence" Nashvile, vanderbillt university Press, 1961.
- MLLUENBACH (L.H.): "Warrantless residential searches to prevent the destruction of evidence: A need for strict standards" The Jouranl of criminal law, criminologm 1979.

وأيضاً: راجع عن التفتيش باللغة الفرنسية:

- STEFANI (G.), LEVASSEUR (G.) et Bouloc (B) "Procédure pénale", Dalloz, 16e édition 1996.
- RASSAT (Michéle-Loure): "Procédure Pénale" P.U.F. 1996.
- SOYER (J.CL.): "Manuel de droit pénal et procédure pénale" I Lé éd.L. G.J. 1994.
- SALAS (D.): "Du procés pénal". P.U.F. 1992.
- PRADEL (J.): "Droit pénal procédure pénale" Tome 2 "Procédure pénale" 7e êd cujas 1993.
- MERLE (R.) et VITU (A.): "Traite de droit criminel" ed. Cujas, tome II, "Procedure penale" 4e ed, 1989.

ومن المؤلفات المتخصصة يراجع:

-/-

أنها تجمع على أن التفتيش(١) عبارة عن:

---

- MELENNEC: "Perquisition, saisies et secret professionnel medical" gaz pal. 1980, I. doctr, 145.
- PRELLE: "La fouille des passagers dans les aeroports: gaz. Pal, 1973, I. doctr.
- GASSIN (R.): "La police judiciaire devant le code de procedure penale: J.R.S.C. 1972.
- MERCIER: "I enquete de flagrant delit" journees police judiciaire, AIX, Mai, 1969.
- BOULOC (B.): "I acted d instruction" these paris, 1965.
- PEDAMON (M>): "La fouille corporelle" R.S.C. 1961, p. 467.
- CREMIEU (L.): "La perquistion chez le bureau d avocet" Rec. dalloz. Juriprudence. 1960, p. 532.

(١) راجع فى تعريف الفقه للتفتيش:

* أنه إجراء من إجراءات التحقيق التى تهدف إلى ضبط أدلة الجريمة موضوع التحقيق وكل ما يفيد فى كشف الحقيقة، وهو ينطوى على مساس بحق المتهم فى سرية حياته الخاصة، (د/ أحمد فتحى سرور – الوسيط فى الإجراءات الجنائية – القاهرة – دار النهضة العربية – ط ٤ – سنة ١٩٨١ ـ ص ٤٤٩).
* وأنه البحث عن الشئ فى مستودع السر، (د/ عوض محمد عوض – المبادئ العامة فى قانون الإجراءات الجنائية – منشأة المعارف – سنة ٢٠٠٢ – ص ٢٨٤).
* وهو البحث فى مستودع أسرار فرد معين عن أدلة تفيد التحقيق بشأن جريمة معينة جناية أو جنحة – وقعت، وتقوم الدلائل الجدية ضد هذا الشخص على ارتكابه لها، وقد يكون مستودع الأسرار محل التفتيش شخص هذا الفرد كما قد يكون أمكنة خاصة له لها حرمتها، (د/ محمود نجيب حسنى – شرح قانون الإجراءات الجنائية – دار النهضة العربية – سنة ١٩٨٨ – ص ٧٧٠).
* وهو وسيلة للإثبات المادى تهدف إلى اكتشاف أشياء خفية أو أشخاص هاربين من وجه العدالة، فهو وسيلة لإثبات أدلة مادية، وقد يكون موضوعه شخصاً أو مكاناً، (د/ أمال عثمان – قانون الإجراءات الجنائية – دار النهضة العربية – رقم ٢٦١ – ص ٣٠٥).
* وهو الإطلاع على محل له حرمة خاصة للبحث عما يفيد التحقيق، ويعتبر من أخطر إجراءات التحقيق الجنائى لأنه يجمع بين استعمال السلطة وتقييد الحرية – وهما من خصائص الإجراءات الاحتياطية كالقبض والحبس – وبين جمع الأدلة، (د/ توفيق الشاوى – فقه الإجراءات الجنائية – دار الكتاب العربى – القاهرة – ط ٢ – سنة ١٩٥٤– ص ٣٧١).

–/–

(إجراء من إجراءات التحقيق التى تهدف إلى البحث عن أدلة مادية لجناية أو جنحة تحقق وقوعها فى محل يتمتع بحرمة المسكن أو الشخص، وذلك من أجل إثبات ارتكابها أو نسبتها إلى المتهم، وفقاً للإجراءات القانونية المقررة)(١).

فيما ذهبت محكمة النقض إلى تعريف التفتيش بأنه: (البحث عن عناصر الحقيقة فى مستودع السر فيها)(٢).

- **أهمية التفتيش:**

التفتيش من أخطر الإجراءات الجنائية التى تمس حريات الناس، فهو بحث فى مستودع أسرارهم التى يحرصون على الاحتفاظ بها لأنفسهم، واعتداء على

---

* وهو إجراء من إجراءت التحقيق تقوم به سلطة حددها القانون، يستهدف البحث عن الأدلة المادية لجناية أو جنحة تحقق وقوعها فى محل خاص يتمتع بالحرمة بغض النظر عن إرادة صاحبه. (د/ سامى الحسينى – مرجع سابق – رقم ٢٨ – ص ٣٧).

* وهو إجراء من إجراءات التحقيق يهدف إلى التوصل إلى أدلة جريمة ارتكبت فعلاً، وذلك بالبحث عن هذه الأدلة فى مستودع السر، سواء أجرى على شخص المتهم أو فى منزله دون توقف على أرادته. (د/ فوزية عبد الستار – الإجراءات الجنائية – القاهرة – دار النهضة – رقم ٢٥٣ – سنة ١٩٩٠ – ص ٢٧٨).

* وهو البحث فى مستودع أسرار الشخص عن أشياء تفيد الغرض من التفتيش، وهو على هذا المعنى وأيا ما كانت أغراضه، مساس بحرية الفرد الشخصية فى حماية أسراره. (د/ محمد ذكى أبو عامر – الإجراءات الجنائية – مكتبة الصحافة – الإسكندرية – سنة ١٩٨٩.

(١) د/ هلالى عبد اللاه أحمد – تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى –مرجع سابق – ص ٤٧.

* ويلاحظ أنه حين يستخدم النظام الأنجلو أمريكى مصطلح واحد للدلالة على تفتيش المسكن وهو Search، نجد أن النظام الفرنسى يغاير فى المصطلح المستخدم فى تفتيش الشخص عنه بالنسبة لتفتيش المسكن:

فهو فى تفتيش الشخص يستخدم مصطلح Fouille a crops أو Fouille corporelle.

أما فى حالة تفتيش المسكن فإنه يستخدم مصطلح Perquistion.

كما يستعمل مصطلح آخر فى حالة دخول المنزل لغرض أخر غير التفتيش هو Visit domi-ciliaire.

(٢) نقض ٣١ مارس سنة ١٩٥٩ – أحكام محكمة النقض – س ١٠ – رقم ٨٧ – ص ٣٩١، نقض ١٧ سبتمبر سنة ١٩٦٢ – أحكام محكمة النقض – س ١٣ – رقم ٢٠٥ – ص ٨٥٣.

حرياتهم فى صون أسرار مساكنهم وأشخاصهم. ولذلك حرصت الدساتير على رفع بعض أحكام التفتيش إلى مصاف المبادئ الدستورية، خاصة بعد الإعلان العالمى لحقوق الإنسان الذى نصت مادته الثانية عشر على أنه: «لا يعرض أحد لتدخل تعسفى فى حياته الخاصة أو أسرته أو مسكنه أو مراسلاته أو لحملات على شرفه وسمعته، ولكل شخص الحق فى حماية القانون من مثل هذا التدخل أو تلك الحملات»(1).

ونتبين من نصوص دستور ٧١ الحالى المادتين ٤١، ٤٤، وجود ضمانات معينة احاطها المشرع المصرى بإجراء التفتيش تعكس مدى أهميته وخطورته على الحريات.

**ثانياً: خصائص التفتيش:**

يتميز إجراء التفتيش بعدة خصائص نجملها فيما يلى(2):

- **أنه إجراء من إجراءات التحقيق:** يجمع الفقه فى مصر على اعتبار أمر التفتيش من أوامر التحقيق الابتدائى وليس من إجراءات الاستدلال، فهو من الأوامر القضائية بلا شبهة، وقد عبر المشرع الإجرائى المصرى عن ذلك فى المادة ١/٩١ معدلة بالقانون رقم ٣٧ لسنة ١٩٧٢ والخاصة بتفتيش المنازل حيث نصت على أن: «تفتيش المنازل عمل من أعمال التحقيق، ولا يجوز الالتجاء إليه إلا بمقتضى أمر من قاضى التحقيق بناء على اتهام موجه إلى شخص يقيم فى المنزل المراد تفتيشه، بارتكاب جناية أو جنحة أو باشتراكه فى ارتكابها، أو إذا وجدت قرائن تدل على أنه حائز لأشياء تتعلق بالجريمة».

ويلاحظ هنا أنه إذا كان النص السابق ورد بخصوص تفتيش المنازل إلا أنه لا يعنى استبعاد تفتيش الأشخاص من نطاق أعمال التحقيق، لأن اعتبار التفتيش

(١) د/ عبد الرءوف مهدى – شرح القواعد العامة للإجراءات الجنائية – دار النهضة العربية – القاهرة – سنة ٢٠٠٢ – ص ٤٣٥.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٤٨ وما بعده، وأيضاً يراجع لذات المؤلف: المركز القانونى للمتهم – مرجع سابق – ص ٥٦٦ وما بعده.

عمل من أعمال التحقيق لا يحتاج إلى نص يقرره[1]. ومصداقاً لذلك نجد أن الفقه الفرنسي يجمع على أن التفتيش عمل من أعمال التحقيق، بالرغم من أن قانون الإجراءات الجنائية الحالي لا يتضمن نصاً بهذا الشأن يقابل نص المادة ٨٧ من قانون التحقيق الجنائي الملغي، التي كانت تقرر أن التفتيش يعد من إجراءات التحقيق[2].

ولا يقوم بإجراء التفتيش إلا سلطة من السلطات المختصة بالتحقيق أو بأمر منها، فالتفتش ذاته ليس بدليل وإنما وسيلة للحصول على الدليل[3].

- **أنه يهدف إلى البحث عن أدلة مادية:** الغرض من التفتيش هو الوصول إلى الأدلة المادية للجريمة. والأدلة المادية هي التي تنبعث من عناصر مادية ناطقة بنفسها وتؤثر في اقتناع القاضي بطريق مباشر. فقد يترك الجناة في مكان الجريمة بعض الأدوات التي استخدمت في ارتكابها أو بصمات أصابع أو آثار أقدام أو غير ذلك من الظواهر المادية التي تفيد في الإثبات، ويلاحظ أن الحصول على هذه الأدلة المادية كما قد يكون بالتفتيش فأنه قد يكون عن طريق المعاينة أو الضبط أو الخبرة. وهذا النوع من الأدلة يختلف عما يطلق عليه الأدلة القولية أو الشفوية[4].

---

(١) وهذا ما سارت عليه المادة ٩٥ من مشروع قانون الإجراءات المصري الجديد، وقد جاء بالمذكرة الإيضاحية اعتبار التفتيش من أعمال التحقيق لا يحتاج إلى نص.

(2) Escande: "Transports Perquistionset saisies" Jur clas proe. pénale art, 92.

(3) Merle et vitu: Traite de droit criminel, Paris, 1967, No, 764, p. 738.

(٤) الأدلة القولية هي: تلك التي تنبعث من عناصر شخصية تتمثل فيما يصدر من الغير من أقوال، وتؤثر في اقتناع القاضي بطريق مباشر من خلال تأكده من صدق هذه الأقوال. والأدلة الشفوية هي: اعتراف المتهم ويتم عن طريق الاستجواب وشهادة الشهود، وتجئ من أقوال من لديهم معلومات في شأن الجريمة محل التحقيق، وبذلك يختلف التفتيش عن الاستجواب وشهادة الشهود.

• ان تكون هذه الأدلة ناشئة عن جناية او جنحة تحقق وقوعها، لا يتخذ إجراء التفتيش بوصفه عملاً من أعمال التحقيق إلا بصدد جريمة قد ارتكبت بالفعل. فلا يصح القيام به لضبط جريمة مستقبلية(١)، ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل(٢). بيد أنه لا يكفى مجرد وقوع جريمة ما للقول بجواز إجراء التفتيش بل لابد أن تكون ما يعتبرها القانون جناية أو جنحة، وبالتالى تستبعد المخالفات. وذلك لأن المخالفات من ضآلة الشأن بحيث لا يتوافر لها من الخطورة، ما يبرر أهدار الحرية الفردية وحرمة المساكن عن طريق إجراء التفتيش(٣).

ويستفاد هذا الشرط من نص المادة ٩١ من قانون الإجراءات الجنائية المصرى، والتى تمنع قاضى التحقيق من اللجوء إلى التفتيش إلا بناء على تهمة موجهة إلى شخص يقيم بالمنزل المراد تفتيشه بارتكاب (جناية أو جنحة)(٤).

---

(١) نقض ١٤ يناير سنة ١٩٨٦ – مجموعة أحكام النقض – سنة ٥٥ – رقم ١٤ – ص ٦٤، نقض ١٦ يناير سنة ١٩٨٦ – مجموعة أحكام النقض – سنة ٥٥ – رقم ٢١ – ص ٩٤، نقض ١٨ ديسمبر سنة ١٩٨٦ – مجموعة أحكام النقض – سنة ٥٦ – رقم ٢٠٦ – ص ١٠٨٥.

* ويراجع كذلك: د/ عوض محمد عوض – مرجع سابق – ص ٢٨٤، (فلا يجوز اللجوء إلى التفتيش للتحقيق من جريمة يخشى وقوعها، وقد حرص المشرع على تقييد التفتيش بهذا القيد، فصرح بذلك فى المادة ١/٥٠ إ – جـ).

(٢) نقض ٣٠ يونيه سنة ١٩٦٩ – مجموعة أحكام النقض – سنة ٢٠ – رقم ١٩٣ – ص ٩٧٣، نقض ١٦ أكتوبر سنة ١٩٦٧ – مجموعة أحكام النقض – سنة ١٨ – رقم ١٩٥ – ص ٩٦٥، نقض ٧ فبراير سنة ١٩٦٧ – مجموعة أحكام النقض – سنة ١٨ – رقم ٣٤ – ص ٩٧٤، نقض أول يناير سنة ١٩٦٢ – مجموعة أحكام النقض – سنة ١٣ – رقم ٥ – ص ٢٠.

(٣) د/ حسن صادق المرصفاوى مرجع سابق – ص ٢٠٥.

(٤) وكذلك كان هذا الشرط مستفاد من أحكام المادة ٤٧ إ – جـ والتى حكم بعدم دستوريتها (حكم المحكمة الدستورية العليا – بتاريخ ٢ يونيه سنة ١٩٨٤).

فقد كانت هذه المادة تجيز لمأمور الضبط القضائى فى حالة التلبس بجناية أو جنحة تفتيش منزل المتهم. وتجدر الإشارة فى هذا الصدد أن مشروع قانون الإجراءات الجنائية الجديد المصرى قد أغفل تحديد وصف الجريمة سواء عند بيانه سلطة أعضاء الضبط القضائى فى

=/=

وعلى الرغم من أن المُشرع الإجرائى الفرنسى لم يذكر نوع الجريمة التى تبيح إجراء التفتيش، إلا أن القضاء لا يجيز إجراءه إلا إذا كانت عقوبة الجريمة مما يقيد الحرية أو يمس بالشرف(١).

• **أن يكون موضوع التفتيش محلاً يتمتع بحرمة المسكن أو الشخص:** ينبغى أن يكون موضوع التفتيش محلاً يتمتع بحرمة المسكن أو الشخص. ومن هنا تتضح أهمية المحل الذى يجرى فيه، فهذا المحل هو ما يميز التفتيش بمفهومه القانونى عن التفتيش بمفهومه العام. ولذلك فإن ما يقوم به رجال الشرطة من مأمورى الضبط القضائى من بحث فى الصحراء أو فى الطرق العامة أو فى المزارع أو فى الترع والبحيرات، لا يعد تفتيشاً بالمعنى المقصود فى قانون الإجراءات لانتفاء حرمة المكان، وإنما هو إجراء من إجراءات الاستدلال يدخل فى صميم اختصاصهم الأصيل(٢).

• **أن يتم التفتيش وفقاً للإجراءات القانونية المقررة:** يجب أن يتم إجراء التفتيش وفقاً للضوابط القانونية التى وضعها المشرع الإجرائى فى هذا الشأن(*).

---

= تفتيش منزل المتهم عند التلبس (المادة ٧٠)، أو عند تناوله سلطة النيابة العامة فى تفتيش المنازل (المادة ٩٥)، واكتفى بإطلاق وصف الجريمة. غير أن ذلك لا يعنى أن المشروع قد قصر إباحة إجراء التفتيش فى المخالفات لأن وصف الجريمة فيه يقتصر على الجنايات والجنح. وقد جاء بالمذكرة الإيضاحية للمشروع أنه: «اتساقاً مع ما أخذ به مشروع قانون العقوبات من تقسيم الجرائم مستبعداً المخالفات من نطاقها، فقد عنى المشروع بوضع نظام إجرائى مستقل للمخالفات يساير انحسار وصف الجريمة عنها دون إخلال بالضمانات الأساسية. وقد افرد المُشرع لهذا التنظيم كتاباً مستقلاً، هو الكتاب الأخير منه، بحيث لا يرجع إلى ما ورد به من أحكام فى شأن المخالفات إلا فيما يحال إليه صراحة».

(1) Cass crim, 18 Fév, 1910 Bull crim, No. 73.

(٢) د/ عوض محمد عوض – المرجع السابق – ص ٢٨٤.

(*) عندما يمارس مأمور الضبط القضائى إجراء التفتيش بناء على حالة التلبس، فانه لابد من توافر بعض الشروط الموضوعية لهذا الإجراء كاختصاص استثنائى تلقائى له، وهذه الشروط تكمل خصائص التفتيش السابق عرضها عامة، وتتمثل هذه الشروط فى:

=/=

**ثالثاً: الطبيعة القانونية لإجراء التفتيش:**

خلصنا مما سبق عرضه إلى أن التفتيش يعتبر إجراء من إجراءات التحقيق، وليس من إجراءات الاستدلال، وعلى ذلك أجمع الفقه فى مصر وفى فرنسا.

لكن متى يعتبر الإجراء الخاص بالتفتيش من أعمال التحقيق.

هل وفقاً للغاية المتوخاه منه؟

أم حسب الوقت الذى تم فيه الإجراء؟

أم تبعاً لصفة القائم به (هل هو عضو نيابة أو ضابط شرطة) ؟

وقد اختلف الفقه عند أجابته على هذه التساؤلات إلى اتجاهات أربع. ولكن قبل أستعرض هذه الاختلافات الفقهية، من الضرورى توضيح أهمية بيان الطبيعة القانونية لإجراء التفتيش والمتمثلة فى: أن ضابط الشرطة عند قيامه بإجراء قانونى فى أطار عمله كمأمور للضبطية القضائية، لابد أن يكون على علم بالطبيعة القانونية لهذا الإجراء، حتى يؤديه بالشكل القانونى المحدد له، دون أن يتجاوز فى الإجراء أو ينتقص منه فيصيبه البطلان. وهذا أمر يؤثر بالسلب على العمل القانونى بأكمله.

- **الاتجاهات الفقهية بشأن الطبيعة القانونية لإجراء التفتيش[1]:**

- **الاتجاه الأول:** يرى أنصار هذا الاتجاه الاعتداد بمعيار الغاية من الإجراء، وعلى ذلك يعتبر التفتيش من إجراءات التحقيق لأنه يتجه إلى

---

- وقوع جريمة فى حالة تلبس.
- أن تكون الجريمة من نوع الجناية أو الجنحة.
- توافر الدلائل الكافية على نسبة الجريمة إلى المتهم.
- يبرر التفتيش الاعتقاد بوجود أدلة مادية تتعلق بالجريمة المرتكبة.

(١) د/ هلالى عبد اللاه أحمد – المركز القانونى للمتهم – مرجع سابق – ص ٥٧٠ وما بعدها.

البحث عن الأدلة وجمعها. ويمثل هذا الاتجاه غالبية الفقه والقضاء فى فرنسا(١).

- الاتجاه الثاني: يأخذ أصحاب هذا الاتجاه بالإضافة إلى الغاية من الإجراء. التوقيت الزمني الذى تم فيه، فإذا كان الإجراء قد اتخذ قبل فتح التحقيق كان من إعمال الاستدلال. أما إذا تم الإجراء بعد فتح التحقيق فانه يعد عملاً من أعمال التحقيق(٢).

- الاتجاه الثالث: يعول القائلون بهذا الاتجاه على صفة القائم بالإجراء، فيعتبر الإجراء من أعمال التحقيق إذا قامت به سلطة التحقيق المنوط بها القيام به دون غيرها(٣). وقد تعرض هذا الاتجاه لعدة انتقادات على أساس أن المشرع الإجرائى لا يعتد بصفة القائم بالإجراء(٤).

كذلك كيف يمكن وصف الإجراء بأنه من أعمال التحقيق، إذا كان القائم به مأمور الضبط القضائى وعلى الأخص فى حالتى التلبس والندب.

لكن يرد على هذا بأن مأمور الضبط القضائى حين يمارس إجراء التفتيش فى حالتى التلبس والندب، فإن القانون يتيح له اتخاذ إجراءات تحقيق لا

---

(١) راجع فى تفصيل هذا الاتجاه:

- BOULOC (B.): "L'Acte d'instruction" Thése, Paris 1965, No 42, p. 26.

ومن أحكام محكمة النقض الفرنسية يراجع:

Cass. Crim. 24 Janv. 1963, Bull, crim, No. 42.

Cass. Crim. 10 Avril, 1959, Bull, crim, No. 206.

Cass. Crim. 26 Janv, 1955, Bull, crim, No. 154.

(2) FREJAVILLE et SOYER: "Manuel de droit Criminal "Paris 1960, No. 357, p. 367.

(٣) راجع فى تفاصيل هذا الاتجاه رسالة بلوك:

BOULOC (B.): These citee, Nos 320 - 328, pp. 218-228.

(4) FREJAVILE et SOYER: op. cit., No. 357, p. 367.

استدلال، ويخضعه لقواعد معينة لا يخضع لها أصلا بوصفه من مأمورى الضبط القضائي[1]. وعلى ذلك فإن المشرع يسبغ على مأمورى الضبط القضائى عندئذ صفة سلطة التحقيق[2].

- **الاتجاه الرابع:** يأخذ أصحاب هذا الاتجاه بالمعايير الثلاثة السابقة تحت تسمية جديدة هى: (**المعيار المختلط**)، فيعتبر العمل من إجراءات التحقيق متى اتخذته سلطة تحقيق، بعد تحريك الدعوى الجنائية بقصد الكشف عن الحقيقة[3]. وبهذا الاتجاه أخذت محكمة النقض المصرية، ويتبدى ذلك فى قولها إن «التفتيش بحسب الأصل إجراء من إجراءات التحقيق لا تأمر به إلا سلطة من سلطاته، لمناسبة جريمة – جناية أو جنحة – ترى أنها وقعت وصحت نسبتها إلى شخص معين، وأن هناك من الدلائل ما يكفى للتعرض لحرية المتهم أو لحرمة مسكنه»[4].

**رابعاً: صور التفتيش:**

انقسم الرأى بين الفقهاء حول نطاق حق تفتيش المتهم، المقرر بنص المادة ١/٤٦ إجراءات جنائية:

- **فذهب رأي إلي القول:** أنه حق عام ثابت لمأمور الضبط فى الأحوال التى يجوز فيها القبض على المتهم، وذلك للبحث عن أدلة الجريمة التى فى حيازته وضبطها، وكذلك لتجريده مما يحتمل أن يكون معها من سلاح، خشية أن يستعمله فى المقاومة أو فى الاعتداء به على نفسه أو على غيره[5].

---

(١) د/ رءوف عبيد – مبادئ الإجراءات الجنائية – دار الفكر العربى – القاهرة – ط ١٧ – سنة ١٩٨٩ – ص ٣٢٦.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٥٧٢.

(٣) د/ سامى حسنى الحسينى – مرجع سابق – ص ٥٥.

(٤) نقض ١٨ يناير سنة ١٩٦٠ – مجموعة أحكام النقض – س ١١ – رقم ١٢ – ص ٧٠.

(٥) د/ محمود محمود مصطفى – مرجع سابق – فقرة ١٧٠ – ص ٢٢١.

ويتفق أستاذنا/ على زكى العرابى مع هذا الرأى أيضاً لأنه يطلق حق التفتيش عند القبض على

-/-

والتفتيش للبحث عن أدلة الجريمة فى حيازة المتهم هو التفتيش المعتبر بحسب الأصل من إجراءات التحقيق Foulille acte d'instruction، أما التفتيش للبحث عما قد يحمله المتهم من سلاح للمقاومة أو للاعتداء به فلا يقصد به إلا أمكان تنفيذ القبض فحسب، فهو إجراء وقائى أو محض بوليسى Fouille-Mesure de police.

- وذهب رأي أخر إلي، أن التفتيش الوقائى أو البوليس هو وحده الذى يجوز لضابط الشرطة أن يجريه على شخص المتهم عند القبض عليه بعيداً عن حالة التلبس، أما التفتيش للبحث عن أدلة الجريمة وضبطها فلا يجوز له فى هذه الحالة(١).

---

= المتهم بمقتضى المادة ٤٦ إ-جـ ولا يقصره على التفتيش البوليسى كما يذهب الرأى المقابل. راجع: الأستاذ/ على زكى العرابى – المرجع السابق – جـ١ – فقرة ٥٣٤ – ص ٣٧٤، ٣٧٥، وكذلك الأستاذ/ عدلى عبد الباقى – شرح قانون الإجراءات الجنائية – المطبعة العالمية – القاهرة – ١٩٥١، جـ١، ص ٣٣٤، د/ عمر السعيد رمضان – مبادئ الاجراءات الجنائية – دار النهضة العربية – ١٩٨٥ – فقرة ١٣٩ – ص ٢٤٤، ٢٤٥، د/ أحمد فتحى سرور – مرجع سابق – فقرة ٢٦٦ – ص ٤٥٤، د/ مأمون محمد سلامة – الإجراءات الجنائية فى التشريع المصرى – دار الفكر العربى سنة ١٩٧٣ – ص ٣٦٣، ٣٦٤.

(١) د/ توفيق محمد الشاوى – مرجع سابق – ص ٢٨٣، وأيضا يراجع بحث للدكتور/ الشاوى فى التفتيش منشور فى مجلة المحاماة – س ٣٢ – عدد ٨ – ص ١٢٠٠، وراجع د/ رءوف عبيد – المرجع السابق –ص ٣٤٥ و ٣٤٥.

حيث يضيف أستاذنا الدكتور/ رءوف عبيد: أن هذا الرأى – رأى الدكتور/ توفيق الشاوى – له مزية تحقيق ضمان هام لمصلحة المتهمين لما يرمى إليه من تقييد حرية مأمور الضبط القضائىَ فى تفتيش الأشخاص فى غير حالة التلبس، بإنكار حقه فى التفتيش بحثاً عن أدلة الجريمة. لكنه لا يمثل نية للمشرع واضع نص المادة ١/٤٦ إ.جـ الواضحة فى أطلاق عبارة المادة والتى تقرر فى غير ما تقييد ولا تخصيص «أنه فى الأحوال التى يجوز فيها القبض على المتهم يجوز لمأمور الضبط القضائى أن يفتشه».

وأيضاً يراجع فى النقد وتنفيد رأى د/ الشناوى باستفاضة: د/ رءوف عبيد – المشكلات العملية الهامة فى الإجراءات الجنائية – مرجع سابق – ص ٩٤، ٩٥.

• فيما ذهب رأي فقهي من الرواد إلى[1]، أن مفتاح المشكلة في نظرنا هو التفرقة بين التفتيش القضائى(*)، وهو التفتيش بالمعنى القانونى، وبين التفتيش الوقائى[2] التابع للقبض وهو الذى قصدته المادة ١/٤٦ ، والذى تقصده محكمة النقض المصرية عندما تقرر أن التفتيش يتبع القبض.

فلا بد من التمييز بين نوعين من تفتيش الشخص:

• النوع الأول، وهو الذى يجب أن يسمى وحده تفتيشاً بالمعنى القانون المعروف فى القانون الجنائى، أى الإطلاع والبحث عن الأدلة، وهو الذى يعتبر (من أعمال التحقيق التى لا يجوز الالتجاء إليها إلا فى تحقيق مفتوح) طبقاً لنص المادة ٩١ إجراءات، ولا يمكن أن تجريه سلطة التحقيق إلا متى توفرت لديها قرائن قوية، على أن فى إجرائه فائدة فى (الإثبات)(**).

---

(١) الأستاذ/ أحمد عثمان حمزاوى – مرجع سابق – ص ٢٨٩.

(*) أخذ بهذه التسمية (جارو) جـ٣ رقم ٩٠٠، ص ٢٠٤، وموريز تيبولت، ص ٤٤٧، و (لويس لامبير) فى البوليس القضائى، جـ١، ص ٣٥١، وبعض الفقهاء يفضل تسميته (التفتيش التحقيقى Fouill-acte d'instruction). مشار إليه لدى: الأستاذ/ أحمد حمزاوى – المرجع السابق – هامش ١ – ص ٢٨٩.

(٢) الأستاذ/ أحمد عثمان حمزاوى – المرجع السابق – ص ٢٨٩.

ويضيف: هذه تسمية استحدثناها، وهى غير موجودة فى الفقه المصرى، ولكننا أخذناها عن عبارات بعض أحكام النقض المصرية مثل: نقض ١١ يونيه سنة ١٩٤٥ حيث وصفت هذا التفتيش بأنه: «من وسائل التوقى والتحوط الواجب توفيرها أماناً من شر المقبوض عليه» – مجموعة النقض جـ٦ – رقم ٥٨٩، ص ٧٣٣، وهذا فى نظرنا أفضل من تسمية التفتيش البوليس التى أخذ بها القضاء الفرنسى فى بعض أحكامه.

(**) لذلك اشترطت المادة ١/٩١ لإجراء التفتيش بمعرفة قاضى التحقيق «أن توجد قرائن على أنه – صاحب المنزل – حائز لأشياء تتعلق بالجريمة».

وبالنسبة للشخص اشترطت مادة ٩٤ إ.جـ: «أن تتضح من أمارات قوية أنه يخفى أشياء تفيد فى كشف الحقيقة».

وبالنسبة لضبط المراسلات التليفونية أجازته م ١٩٥ إ.جـ: «متى كان لذلك فائدة فى ظهور الحقيقة».

• **أما النوع الثاني**، وهو الذى يكون تابعاً للقبض على الأشخاص، فهو الذى أسميناه (تفتيشاً وقائياً) وهو ليس من إجراءات التحقيق، ولا يقصد به البحث عن أدلة، وإنما هو إجراء بوليسى محض مقصود به أمكان تنفيذ الأمر بالقبض(*). وهو لذلك محدد بحدود هذه الغاية ولا يجوز أن يتعداها(**).

• **رأي محكمة النقض في الموضوع**، رددت محكمة النقض فى أحكامها التى صدرت فى ظل القانون الحالى القول بأن: «التفتيش الذى يجريه مأمور الضبط القضائى على من يقبض عليه هو إجراء صحيح من إجراءات الاستدلالات التى تلزم للتحقيق وفقاً للمادة ٤٦ ...، والقول بأن التفتيش المشار إليه فى هذه المادة قصد به التفتيش الوقائى، هو تأويل يقع دون صيغة التعميم التى ورد بها النص، وأحال فيها على الأحوال التى يجوز فيها القبض قانوناً على المتهم»(١)، واضطرد قضاؤها على ذلك، مما لا يدع مجالاً للشك

---

(*) ولذلك فان التفتيش يجوز فى جميع أحوال القبض أياً كان نوع هذا القبض أو سببه أو الغرض منه. (نقض ٢٤ ديسمبر سنة ١٩٤٥ مجموعة النقض جـ٧ - رقم ٤٢ - ص ٣٢)، حتى ولو لم يكن القبض من أعمال التحقيق. بأن كان المقصود منه تنفيذ حكم جنائى مثلاً أو تنفيذ أمر بالحبس الاحتياطى.

(**) أفضل تعريف للتفتيش الوقائى يمكن استخراجه من عبارات محكمة النقض المصرية بأنه هو: «ما يستلزمه تنفيذ القبض من بحث فى ملابس المتهم لتجريده مما يحتمل أن يكون معه من سلاح خشية أن يستعمله فى المقاومة أو الاعتداء على نفسه أو على من يقبض عليه». نقض ٢ يونيه سنة ١٩٤١ مجموعة النقض جـ٥ - رقم ٢٧٣ - ص ٥٣٧.

وبذلك يختلف التفتيش الوقائى عن التفتيش من حيث طبيعته القانونية، إذ أنه ليس إلا إجراء بوليسياً احتياطياً تنفيذياً - ولذلك سمته إحدى المحاكم الفرنسية (التفتيش البوليسى Fouille-mesure de police). محكمة استئناف نيم فى جازيت ديباليه ١٩٢٧ - ١ - ص ١٩٤. (الأستاذ/ حمزاوى - المرجع السابق - ص ٢٩١).

(١) نقض ٢ نوفمبر سنة ١٩٥٤ أحكام النقض س ٦ - رقم ٥ - ص ١٦٢.

وأيضا: يراجع تعليقاً للأستاذ الدكتور/ رءوف عبيد بشأن ذات الحكم - مجلة المحاماة - س ٣٥ - عدد ٩ - ص ١٧٨٥ وما بعدها.

فى أنه يبيح تفتيش شخص المتهم - بحثاً عن أدلة الجريمة لضبطها وهى فى حيازته - ما دام القبض عليه وقع صحيحاً، وذلك استناداً إلى عموم عبارة المادة ١/٤٦ إ - ج[(١)].

**البند الثاني: تفتيش نظم المعلوماتية: -**

يتم إجراء التفتيش للنظم المعلوماتية من خلال الوعاء الذى يحوى هذه النظم ويقصد به جهاز الحاسب الآلى، والذى يتكون كما أوضحنا سلفاً من مكونات مادية Hard ware ومكونات منطقية Soft ware، كما أن له شبكات أتصال بعدته سلكية ولاسلكية Networks tele communication، على المستوى الوطنى والمستوى الدولى[(*)].

وجهاز الحاسب قد يعمل بمفرده أو يعمل من خلال شبكة اتصالات - ويقصد بالشبكة Net work أتصال جهازين أو أكثر من أجهزة الحاسب الآلى أتصالا سلكياً أو لاسلكياً، أو هى حزمة من أجهزة الحاسبات المتصلة معاً. وقد تكون الأجهزة موجودة فى نفس الموقع فتسمى شبكة محلية Local Area Net-

---

(١) نقض ٣٠ ديسمبر سنة ١٨٥٢ - أحكام النقض - س ٤ - رقم ١٢١ - ص ٣١٢. وفى نفس المعنى نقض ١٣ ابريل ١٩٦٤ - س ١٥ - رقم ٥٥ - ص ٢٧٨، نقض ١١ ديسمبر ١٩٦٧ - أحكام النقض - س ١٨ - رقم ٢٦٣ - ص ١٢٤٢، نقض ٥ فبراير ١٩٦٨ - أحكام النقض - س ١٩ - رقم ٢٨ - ص ١٥٦، نقض ١٣ يناير ١٩٦٩ - أحكام النقض - س ٢ - رقم ٢١ - ص٩٦.

(*) تنقسم المكونات المادية للحاسوب إلى ست وحدات: (وحدة المدخلات: «وحدات الادخال» Im-put units، وحدة الذاكرة الرئيسية Main memory، وحدة الحساب والمنطق Arithmetic and logic unit، وحدة التحكم Control unit، وحدة المخرجات (وحدات الإخراج) Out units، وحدة التجزئة الثانوية Secondary storage units.

أما المكونات المنطقية للحاسب Computer software فهى عبارة عن تعليمات مكتوبة بلغة ما موجهه إلى الحاسب بوصفه جهازاً تقنياً معقداً بغرض الوصول إلى نتيجة معينة، وتنقسم برامج الحاسب إلى نوعين: برامج النظام (الكيانات المنطقية الأساسية)، والنوع الثانى برامج التطبيقات (الكيانات المنطقية التطبيقية). (راجع ما تقدم ص ).

work، كما قد تكون موزعة فى أماكن متفرقة، يتم ربطها عن طريق خطوط التليفون ويطلق عليها فى هذه الحالة شبكة واسعة النطاقWide Area Net work .

وفى نطاق تنفيذ مأمور الضبط القضائى لإجراء التفتيش لجهاز الحاسوب لضبط جريمة معلوماتية، يثور تساؤل هام عن مدى خضوع جهاز الحاسوب للتفتيش؟ أو بمعنى آخر هل يمكن تفتيش جهاز الحاسب الآلى؟ وتتم الاجابة على هذا التساؤل من خلال عرض وتحليل الصور الثلاث التالية(١):

**الصورة الأولي: تفتيش مكونات الحاسب المادية:**

واقع الأمر أن ولوج المكونات المادية للحاسب بأوعيتها المختلفة، بحثاً عن شئ يتصل بجريمة معلوماتية قد وقعت، ويفيد فى كشف الحقيقة عنها وعن مرتكبيها، لاخلاف بين الفقهاء فى أنه يدخل فى نطاق التفتيش طالما تم وفقاً للإجراءات القانونية المقررة. بمعنى أن حكم تفتيش تلك المكونات يتوقف على طبيعة المكان الموجودة فيه، وهل هو من الأماكن العامة Lieux Publice أم الأماكن الخاصة Leslieux Privés. إذ أن لصفة المكان أهمية خاصة فى مجال التفتيش - فإذا كانت موجودة فى مكان خاص Un lieu privé كمسكن المتهم أو أحد ملحقاته كان لها حكمه.

فلا يجوز تفتيشها إلا فى الحالات التى يجوز فيها تفتيش مسكنه وبنفس الضمانات المقررة قانوناً فى التشريعات المختلفة.

**وفي داخل المكان الخاص يجب التفرقة بين:**

- ما إذا كانت مكونات الحاسب منعزلة عن غيرها من الحاسبات الأخرى.
- أم أنها متصلة بحاسب آخر، أو نهاية طرفية Terminal فى مكان آخر كمسكن غير مسكن المتهم.

---

(١) د/ هلالى عبد اللاه أحمد - تفتيش نظم الحاسب الآلى وضمانات المتهم المعلوماتى - مرجع سابق - ص ٧٣ وما بعدها.

فإذا كانت هناك بيانات مخزنة فى أوعية هذا النظام الآخر من شأنها إماطة اللثام عن وجه الحقيقة، تعين مراعاة القيود والضمانات التى يوجبها المشرع لتفتيش هذه الأماكن.

- وبالنسبة للأماكن العامة، سواء كانت من الأماكن العامة بطبيعتها Les lieux publice par nature(*) كالطرق العامة والميادين والشوارع والمتنزهات العامة، أم كانت من الأماكن العامة بالتخصيص Les lieux publics par destination(**) كالمقاهى والمطاعم والسيارات العامة.

فإذا وجد الشخص فى هذه الأماكن وهو يحمل مكونات الحاسب سالفة الذكر، أو كان مسيطراً عليها، أو حائزاً لها، فإن تفتيشها لا يكون إلا فى الحالات التى يجوز فيها تفتيش الأشخاص، وبنفس الضمانات والقيود المنصوص عليها فى هذا الصدد.

**أولاً: تفتيش مكونات الحاسب الآلي في نطاق التشريعات المقارنة:**

من التطبيقات التشريعية التى تجيز تفتيش مكونات الحاسب الآلى، من خلال ما تخوله بعض التقنيات الإجرائية لسلطة التحقيق من أتخاذ أى

---

(*) وهى الأماكن التى تستخدم فى مرور الكافة La circulationdu public، أى الأماكن التى يتسنى لكل إنسان أن يمر بها فى كل وقت.

(**) وهى تلك الأماكن التى لا تكون عامة إلا فى أوقات معينة Certains moments، حيث يباح دخولها إما لكل الناس بلا تفرقة، وإما لفئات معينة من الأفراد، وقد تكون بمقابل أو مجاناً.
للمزيد بشأن بيان الأماكن العامة والخاصة فى نطاق أحكام التفتيش يراجع:
أ/ أحمد عثمان حمزاوى – مرجع سابق – ص ٢٧٥ وما بعدها. فى شرح نص المادة ٤٥ من قانون الإجراءات الجنائية المصرى – بند ٦، حيث ذكر.. ويمكن حصر الأحوال التى يجوز فيها لرجال السلطة العامة دخول المنازل والمحلات فيما يلى:
- المحلات العمومية المفتوحة للجمهور. (كالمقاهى – المطاعم – دور التمثيل – السينما – محلات التجارة) حيث يسوغ للجمهور ا لدخول فيها للغرض المخصص لها.
- المحلات المخصصة للصناعة أو للتجارة ويكون عملها تحت ملاحظة البوليس.
- فى حالة الاستغاثة أو طلب المساعدة من الداخل أو الحريق. فى حالة التلبس بالجريمة.

إجراء، أو القيام بأى فعل لازم لجمع أدلة الجريمة والحفاظ عليها، نصوص التشريعات التالية:

- المادة ٢٥١ من قانون الإجراءات الجنائية اليونانى[1].
- المادة ٤٨٧ من القانون الجنائى الكندى[2].

وفى نطاق وجود بعض القوانين التى تقدم قواعد تفصيلية للتفتيش، تطبق على مكونات الحاسب الآلى وبياناته فى حالات معينة. نجد القسم الفرعى رقم ١٦/١ من قانون المنافسة The competition ACT الكندى.

فهذا القسم يزود الشخص الذى يحمل إذناً للتفتيش إمكانية أن يستخدم أو يعمل على استخدام أى نظام للحاسب الآلى، لتفتيش أى بيانات يحتويها أو تكون متاحة لهذا النظام. كما يمكنه أن يسجل أو يعمل على تسجيل تلك البيانات فى شكل مطبوعات، أو أى مخرجات أخرى[3].

- وفى لوكسمبررج يمكن القول بصفة عامة أن التفتيش يشمل كل الأشياء التى تكون مفيدة فى إظهار الحقيقة Tous les objets qui seront jugés utiles à la manifestation de la vérité[4].

---

(1) Vassilaki (Irini): "Computer crimes and other crimes against information technology in Greece". R.I.D.P. 1993, p. 371.

(2) Piragoff (Donald K.): "Computer crimes and other crimes against information technology in canda". R.I.D.P. 1993, p. 241.

(٣) راجع التقرير العام لمؤتمر .A.I.D.P المنعقد سنة ١٩٩٣.

- Durham (Cole): "The Emerging structures of criminal information Law: Tracing the contours of a New Poradigm". R.I.D.P. 1993, p. 111.

(4) Jaeger (Mare): "Les crimes informatiques et d'autres crimes dans le domaine le de la Technologic informatique au Luxembourg", R.I.D.P. 1993, p. 467.

ويلاحظ أن هناك بعض من التشريعات – القليلة – التي تنص صراحة على تفتيش مكونات الحاسب الآلي. ومن ذلك القانون الإنجليزي الصادر في ٢٩ يونيه سنة ١٩٩٠، والذي طبق اعتباراً من ٢٩ أغسطس سنة ١٩٩٠، والذي يطلق عليه قانون إساءة استخدام الحاسب(١) Computer misuse Act، فبالنسبة للجرائم المدرجة في القسم الثاني(*) والقسم الثالث(**) من هذا القانون. والتي يعاقب عليها بعقوبة السجن لمدة لا تتجاوز خمس سنوات، فإن هذه النوعية من الجرائم تجيز القبض على المتهم دون حاجة لإذن قضائي Without warrant، كما تجيز تفتيش محل إقامة المتهم بحثاً عن أدلة مادية ذات قيمة تتعلق بالجريمة محل القبض(***).

---

(١) لمزيد من المعرفة حول هذا القانون يراجع:

- FERBRACHD (David): "Pathology of computer viruses" springer-verlay London, L T D. 1992, p. 233.

(*) وهي جريمة الولوج غير المصرح به على نظام الحاسب الآلي، لتسهيل ارتكاب أفعال غير مشروعة عن قصد، ويعاقب عليها بمدة أقصاها خمس سنوات.

- An offence of unauthorised access with intent to commit or faclitate commission of further offences has also been created which carries a maximum sentence of 5 Year's imprisonment.

(**) وهي جريمة التعديل غير المصرح به في نظام الحاسب، ويعاقب عليها بنفس العقوبات المنصوص عليها في القسم الثاني أعلاه، فالشخص يكون مذنباً إذا قام بأي فعل ينجم عنه تعديل غير مصرح به في محتويات أي حاسب، وكان وقت حدوث الفعل لديه النية والعلم بذلك.

- An offence of unauthorised modification of computer material is Created which Caries the same penalties as the section 2 offence above. A person is guilty of the offence if. (1) he does any act which couses an unauthorised modification of the contenets of any computer and (II) at the time when he does the act he has the requisite intent any the requisite Knowledge.

(***) وذلك عكس ما ذهب اليه قضاء المحكمة الدستورية العليا في القضية رقم ٥ لسنة ٤ قضائية

-/-

أما بالنسبة للجرائم المدرجة فى القسم الأول(*)، والتى يعاقب عليها بالحبس لمدة لا تتجاوز ستة شهور، فإن التفتيش لا يكون إلا بناء على إذن قضائى يستند على أسباب منطقية، للاعتقاد بأن الجريمة قد وقعت أو يشتبه في وقوعها فى أماكن خاصة Particular Premises، وأن ثمة أدلة متعلقة بهذه الجريمة يمكن الحصول عليها فى هذه الأماكن.(**)

**ثانياً: الوضع في التشريع الأمريكي:**

يجب على السلطات الحصول على أذن التفتيش، قبل الحصول على المعلومات المخزنة فى داخل الحاسوب.

ويحد التعديل الرابع (للدستور الأمريكى) من قدرة السلطات على البحث عن دليل بدون أذن تفتيش، وينص هذا التعديل على:

«حق الناس فى أن يكونوا أمنين فى شخوصهم ومنازلهم وأوراقهم وممتلكاتهم ضد التفتيش والاعتقال الغير قانونى. ويجب إلا ينتهك أى من ذلك. ولن يتم اصدار أى أذن ضبط وتفتيش إلا على أساس سبب معقول ومدعوم

---

= دستورية بجلسة ٢ يونيه سنة ١٩٨٤، حيث قضى بعدم دستورية المادة ٤٧ من قانون الإجراءات الجنائيةلتعارضها مع المادة ٤٤ من الدستور التى تنص على أن: «للمساكن حرمة فلا يجوز دخولها ولا تفتيشها إلا بأمر قضائى مسبب وفقاً لأحكام القانون».

(*) وهى جريمة الولوج غير المصرح به لنظام الحاسب (دون ارتباطها بجريمة أخرى) ويعاقب عليها بالحبس مدة أقاصها ستة شهور.

- An offence of unauthorised access to computer material. The offence carries a maximum 6 - month Period of imprisonment.

(**) ويرى البعض أنه ليس من المعتاد إصدار أمر تفتيش بالنسبة لمثل هذه الجريمة البسيطة Summary offence، لكن ربما تكون المشاكل الخاصة بكشف الجريمة هى التى تبرر ذلك.

- WASIK (Martin): "Computer crimes and other crimes against information technology in the united kingdon", R.I.D.P. 1993, p. 640.

بقسم وافادة، موصوف فيها بدقة المكان المقصود تفتيشه والإفراد والاشياء المراد ضبطها.

وطبقاً لما قررته المحكمة العليا فإن التفتيش بدون أذن لا ينتهك التعديل الرابع اذا تحقق واحد من هذين الشرطين[1]:

أولاً: اذا كان سلوك السلطات لا ينتهك التوقع المعقول للخصوصية Reasonable Expectation of Privacy لدى الأفراد، ومن ثم فإن ذلك لا يشكل تفتيشاً رسمياً وفقاً للتعديل الرابع، ولا يتطلب أذناً ما.

ثانياً: التفتيش بدون أذن Warrantless search الذى ينتهك التوقع المعقول للخصوصية لدى الأفراد، يُعد مبرراً ومعقولاً (وبناء على ذلك دستورياً) اذا اندرج فى اطار الاستثناء على الأذن بالتفتيش.

وبناء على ذلك يلتزم المحقق بأن يأخذ أمران فى الاعتبار حال الاستفسار عما إذا كان تفتيش السلطات للحاسوب يتطلب أذناً أم لا.

**الأمر الأول:** هل التفتيش ينتهك التوقع المعقول للخصوصية؟ وإذا كان كذلك.

**الأمر الثاني:** هل يعد التفتيش مع ذلك معقولاً ومبرراً لأنه يقع فى نطاق الاستثناء على الأذن بالتفتيش؟

ويجب على السلطات الحصول على أذن تفتيش قبل الحصول على المعلومات المخزنة فى داخل الحاسوب.

وذلك رداً على سؤال رئيسى مرتبط بالتعديل الرابع فى قضايا الحاسوب، فيما اذا كان الفرد يتمتع بالتوقع المعقول للخصوصية، على المعلومات الالكترونية المخزنة فى الحواسب (أو أية أجهزة تخزين الكترونية أخرى). التى يتحكم فيها الفرد؟

(١) د/ عمر محمد بن يونس – الإجراءات الجنائية عبر الأنترنت (فى القانون الأمريكى) – مرجع سابق – ص ص ٥٥، ٥٦.

فعلى سبيل المثال.. هل لدى الأفراد توقع معقول للخصوصية:

- فى محتويات الحواسيب المحمولة Laptop Computers الخاصة بهم.
- وكذلك الاقراص المرنة Floppy Disks.
- أو أجهزة الاستدعاء Pagers.

وعندما تواجه المحاكم هذه القضية فأنه يجب عليها أن تشبه أجهزة التخزين الالكترونية بالحاويات المغلقة Closed containers، وعليها التسبب من حيث أن الحصول على المعلومات المخزنة داخل جهاز الكترونى، مشابه لفتح حاوية مغلقة.

- التطبيقات القضائية[١]:

**قضية Barth[٢]:**

وجود توقع معقول للخصوصية فى ملفات مخزنة على القرص الصلب Hard Drive لحاسوب شخصىPersonal computer.

**قضية Reyes[٣]:**

وجود توقع معقول للخصوصية فى البيانات المخزنة على جهاز الاستدعاءPager.

**قضية Blas & Chan & Lynch[٤]:**

للفرد ذات التوقع المعقول للخصوصية، فى جهاز الاستدعاء، والحاسوب، أو

(١) المرجع السابق – ص ٦٠.

(2) United states. V. Barth, 26 F. Supp. 2 d 929, 936 - 37 (W.D. tex. 1998).

(3) United States. V. Reyes, 922 f. Supp. 818, 832-33 (S.D. N.T. 1996).

(4) United States V. Lynch, 908 F. Supp. 284, 287 (D.V.I. 1995).
united states V. Chan, 830 f. Supp. 531, 535 (N.D. cal. 1993) (Same); united states V. Blas, 1990 Wl 265179, at 21 (E.D. Wis.Des. 4, 1990).

أى مخزن الكترونى للبيانات، والجهاز الاستردادى Retrieval Device مثل الحاويات المغلقة.

**الصورة الثانية: تفتيش مكونات الحاسب المعنوية:**

أثارت هذه الصورة خلافاً كبيراً فى الفقه المقارن بين مؤيد ومعارض، حيث ذهب رأى إلى أنه إذا كانت الغاية من التفتيش ضبط الأدلة المادية التى تفيد فى كشف الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات الإليكترونية أو قاعدة البيانات بمشتملاتها.

وفى هذا المفهوم تعطى المادة ٢٥١ من قانون الإجراءات اليونانى سلطات التحقيق مكنة القيام بأى شئ يكون ضرورياً لجمع وحماية الإدلة(*).

**الصورة الثالثة: تفتيش شبكات الحاسب:**

عند مدارسة إجراء تفتيش شبكات الحاسب الآلى، فى اطار تنفيذ مأمور الضبط القضائى لهذا الإجراء، يكون ملتزماً بقواعد الشرعية الإجرائية، التى تضفى على إجراءه الصبغة القانونية، وفى هذا النطاق يمكن التمييز بين ثلاثة فروض، بيانها(١):

**الفرض الأول: اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر داخل الدولة:**

يثير هذا الفرض تساؤل هام يتعلق بمدى إمكانية امتداد الحق فى التفتيش، إذا تبين أن الحاسب أو النهاية الطرفية Terminal فى منزل المتهم متصلة بجهاز أو نهاية طرفية فى مكان آخر مملوك لشخص غير المتهم؟

**- في المانيا:**

يرى الفقه أنه يمكن أن يمتد التفتيش إلى سجلات البيانات التى تكون فى

---

(*) سيتم تناول هذه الصورة بالتفصيل عند دراسة ضبط المكونات المعنوية للحاسب الألى، ص

(١) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٧٧.

موقع آخر، استناداً إلى مقتضيات القسم ١٠٣ من قانون الإجراءات الجنائية الألماني، وذلك عندما يكون مكان تخزين البيانات الفعلي خارج المكان ا لذى يتم فيه التفتيش(١).

**وهناك أيضاً تشريعات تعرضت صراحة للرد على هذا التساؤل منها:**

- مشروع قانون جريمة الحاسب The computer crime Bill فى هولندا(٢):

ينص على إمكانية أن يمتد التفتيش إلى الأجهزة المعلوماتية الموجودة فى موقع آخر، شريطة أن تكون البيانات الخاصة به ضرورية لإظهار الحقيقة (القسم الخامس المادة ١٢٥ بفقرتيها J.K)، وذلك مع التقييد بمجموعة من الضوابط منها ما سبق ذكره (الضرورة لإظهار الحقيقة)، وان يكون ا لتدخل مؤقتاًTemporary .

**الفرض الثاني: اتصال حاسب المتهم بحاسب أو نهاية طرفية موجودة في مكان آخر خارج الدولة(٣):**

من المشاكل التى تواجه سلطات الإدعاء فى جمع الأدلة - والتى عرضها الاستاذ Ulirch sieber فى تقريره المقدم لمؤتمر A.I.D.P - قيام مرتكبى جرائم المعلوماتية بتخزين بياناتهم فى أنظمة تقنية المعلومات خارج الدولة، عن طريق شبكة الاتصالات البعدية Telecommunications network بهدف عرقلة التحقيقات(٤).

(1) KASPERSEN (W.K. Henrik): "Computer crimes and other erimes against information tech nology in the Netherlands R.I.D.P. 1993. p. 479.

(2) DURHAM (Cole): op. cit., p. 114.

(٣) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٧٨ وما بعدها.

(4) SIEBER (Ulrich): "Computer crimes and other crimes against information Technology" - Commentary and Preparatory questions for the colloquium of the A.I.D.P. in Wurzburg. R.I.D.P. 1993, p. 77.

ولمواجهة هذا التكنيك المتطور لتخزين المعلومات، بدأت بعض النظم القانونية فى التصدى له، من هذه النظم:

- في هولندا:

مشروع قانون جريمة الحاسب The Computer Crime Bill يصرح لجهات التحقيق بإجراء التفتيش داخل الأماكن بما يتضمن تفتيش نظم الحاسب المرتبطة حتى إذا كانت موجودة في دول أخرى، وذلك بشرط أن يكون هذا التدخل مؤقتاTemporary، وأن تكون البيانات التي يتم التفتيش عنها لازمة لإظهار الحقيقة (المادة ١٢٥/J)(١).

ويتحفظ جانب من الفقه الهولندى على نص المادة ١٢٥/J سالفة الذكر، بالقول بإنه قد يكون من الأفضل لأسباب عملية، السماح بالتفتيش لنظام الحاسب الموجود فى بلد أجنبى بغرض ضبط البيانات المخزنة فيه، بيد أن هذا الاختراق المباشر Direct Penetration وفقاً لتقرير المجلس الأوروبى The council of Eu-ropraport يعتبر انتهاكاً لسيادة دولة أخرى، ولذا فإنه مع عدم وجود اتفاقية دولية فإن هذا الاختراق المباشر الذى تتضمنه المادة ١٢٥/J يفضل عدم تطبيقة(٢).

- في ألمانيا:

يجد رأى – عدم تفتيش نظام الحاسب الموجود فى بلد أجنبى – إرهاصاته فى المانيا، إذ يتشكك بعض الفقهاء الألمان فى مسألة الولوج إلى أنظمة تقنية

(1) DURHAM (Cole): op. cit., p. 115.

(2) KASPERSEN (W.K.Henrik): op. cit., pp. 503-504.

ولذا فان السائد فى هولندا نظام «التفويض الالتماسى Letters rogatory»، وذلك لحث سلطات الدولة الأخرى على نسخ البيانات الموجودة فى أراضيها وإرسالها إلى السلطات الهولندية مع المعاملة بالمثل، وان كان هذا النظام يعيبه عدم الفاعلية والبطء مما يؤثر سلباً على عملية جمع الأدلة والمحافظة عليها.

- Ibid., p. 503.

المعلومات الأجنبية لضبط البيانات المخزنة فيها(١)، بقولهم: ان السماح باسترجاع البيانات التى تم تخزينها بالخارج، وخاصة عندما يكون ذلك الاسترجاع مرتبطاً بالوضع القائم لحساب فى بنك أمر مشكوك فيه. وأنه فى ظل غياب الاتفاق الخاص بين الدول المعنية، قد يعتبر ذلك خرقاً لحقوق السيادة لدولة أخرى، وخرقاً للقوانين الثنائية والوطنية الخاصة بإمكانية التعاون فى مجال العدالة القضائية(٢).

ويؤيد هذا الرأى التطبيق القضائى فى ألمانيا، ففى إحدى قضايا الغش المعلوماتى، اسفر البحث عن وجود نهاية طرفية حاسب Computer terminal فى ألمانيا متصلة بشبكة اتصالات فى سويسرا حيث يتم تخزين بيانات المشروعات فيها. فلما أرادت سلطات التحقيق الألمانية الحصول على هذه البيانات، لم يتحقق لها ذلك إلا من خلال التماس المساعدة المبتادلة Request for mutual assistance(٣).

- في المجر:

يرى الفقه هناك أن لجوء الجناة إلى تخزين بيانات بالخارج بهدف عرقلة التحقيقات، لا يثير مشكلة على أساس أن الشرطة المجرية مشتركة فى شبكة اتصالات الانتربول The telecommunication networke of interpol(٤).

---

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٧٩.

(2) MOHREN SCHLAGER (Manfred): op. cit., p. 351.

(3) Ibid., p. 356.

(4) KERTESZ (Imre) and PUSZTAI (Laszlo): Computer crimes and other Crimes against information Technology in Hungary. R.I.D.P. 1993, p. 387.

**الفرض الثالث: التنصت والمراقبة الإلكترونية لشبكات الحاسب الآلي:**

التنصت(*) والأشكال الأخرى للمراقبة الإليكترونية رغم أنها مثيرة للجدل، إلا أنه مسموح بها تحت ظروف معينة فى معظم الدول تقريباً(١).

**- في فرنسا:**

يجيز قانون ١٠ يوليو سنة ١٩٩١ اعتراض الاتصالات البعدية، بما فى ذلك شبكات تبادل المعلوماتLes réseaux d'echanges de données (٢).

**- وفي هولندا:**

يجوز لقاضى التحقيق أن يأمر بالتنصت على شبكات اتصالات الحاسب، اذا كانت هناك جرائم خطيرة ضالع فيها المتهم، وتشمل هذه الشبكات التلكس Telex والفاكس Telefax ونقل البيانات Data Communication (**).

**- وفي فنلندا:**

يجوز للشرطة التنصت على المكالمات التلفونية الخاصة بشبكات الحاسب بمقتضى إذن يقدم فى كل حالة على حدة(٣).

---

(*) التنصت Espionnage:
يقصد به مراقبة المحادثات التليفونية وتسجيلها بالنسبة للأحاديث الخاصة بشخص أو أكثر مشتبه فيه، ويعتقد بفائدة محادثاته فى الكشف عن الحقيقة، وذلك عن طريق إخضاعها لنوع من الرقابة بقصد التعرف على مضمونها. (د/ هلالى عبد اللاه أحمد – المركز القانونى للمتهم – مرجع سابق – ص ٦٧٠).

(1) DURHAM (Cole): op. cit., p. 113.

(2) FRANCILLON (jacques): "Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France" R.I.D.P. 1993, p. 309.

(**) ويلاحظ أنه اذا كان التنصت على اتصالات مشفرة Encrypted telecommuni cation مشروع قانون جرائم الحاسب The computer crime Bill – لا يعطى للشرطة أى صلاحيات لفك هذه الرموز وقت تسجيلها، حتى يمكن معرفة ما إذا كانت هذه المعلومات تتعلق بالتحقيقات الجنائية من عدمه. يراجع:
KASPERSEN (W.K. Henrik) op, cit., pp. 500 - 501.

(3) PIHLAJAMAKI (Antti): "Computer crimes and other crimes against information technology in Finland. R.I.D.P. 1993. p. 286.

- وفي كندا:

فإن القوانين العادية التى تهيمن على المراقبة الإليكترونية، يمكن أن تطبق على أنواع عديدة من اتصالات الحاسب الآلى(١).

- وفي اليابان:

أقرت محكمة مقاطعة Kofu سنة ١٩٩١ – فى ظل عدم وجود نصوص تشريعية – شرعية التنصت على شبكات الحاسب للبحث عن دليل(٢).

**البند الثالث: ضوابط تفتيش نظم المعلوماتية:**

**أولاً: الضوابط العامة للبحث عن الحقيقة:**

إذا كان الوصول إلى الحقيقة يمثل الغاية من الإجراءات الجنائية، بيد أن تحقيق هذه الغاية لا يكون بأى ثمن. ففى كل الحالات فإن الغاية لا تبرر الوسيلة... "En Aucune Circonstance la Fin ne saurait Justifier Les moy-ens" هذه الحكمة القديمة تعنى – فى مجال دراستنا – أن البحث عن الحقيقة القضائية La vérité Judiciaire لا ينبغى أن يكون طليقاً من كل قيد، بل إن ذلك يخضع لضوابط معينة حتى لا يتعسف من يسعى للحصول عليها أو يضل. ومن هذا المنطلق حرصت المواثيق الدولية وإعلانات الحقوق والمؤتمرات الدولية والاقليمية، على النص على مجموعة من القيم الأساسية التى ينبغى مراعاتها والأخذ بها(٣).

ولقد أولى ميثاق الأمم المتحدة اهتماماً ملحوظاً بموضوع حقوق الإنسان وحرياته الأساسية فى أطار أقرار العدالة والبحث عن الحقيقة حيث أفرد لذلك

---

(1) PIRAGOFF (Donald K.), op. cit.

(2) YAMAGUCHI (Atsushi): "Computer crimes and other crimes... in Japan" R.I.D.P. 1993, p. 448.

(٣) د/ هلالى عبد اللاه أحمد – تفتيش نظم الحاسب وضمانات المتهم المعلوماتى – مرجع سابق – ص ٩٣.

العديد من النصوص القانونية، تعد المادة الثانية منه – هى الأهم فى بحثنا – واضعه لاحد أهم ضوابط البحث عن الحقيقة، حيث تقرر أن أغراض هذه المنظمة تطوير وتشجيع احترام حقوق الإنسان وحرياته الأساسية(*).

وفى ذات السياق حرصت الاتفاقية الأوروبية لحقوق الإنسان(**) La conven-

---

(*) جاء فى ديباجة ميثاق الأمم المتحدة ما يلى: «نحن شعوب الأمم المتحدة، وقد ألينا على أنفسنا... وأن نؤكد من جديد ايماننا بالحقوق الاساسية للإنسان وبكرامة الفرد وقدره وبما للرجال والنساء والأمم كبيرها وصغيرها من حقوق متساوية».

وتقضى المادة (٦٥) من الميثاق بوجوب أن تعمل الأمم المتحدة على أن: «يشيع فى العالم احترام حقوق الإنسان والحريات الأساسية للجميع بلا تمييز بسبب الجنس أو اللغة أو الدين، ولا تفريق بين الرجال والنساء، ومراعاة تلك الحقوق والحريات فعلاً».

وفى إطار هذا الميثاق أصدرت الجمعية العامة للأمم المتحدة فى ١٠ ديسمبر سنة ١٩٤٨ الإعلان العالمى لحقوق الإنسان La déclaration universelle des Droits de L'homme. الذى نص فى مادته الثالثة على أن: «لكل فرد الحق فى الحياة والحرية وسلامة شخصه».

ونص فى مادته الخامسة على حظر تعذيب أى شخص أو إخضاعه لأية عقوبات أو معاملات وحشية أو تلك التى تحط من أدميته.

ونص فى المادة العاشرة على أن: «لكل انسان الحق على قدم المساواة التامة مع الأخرين، أن تنظر قضيته أمام محكمة مستقلة نزيهة، نظرا عادلاً علنيا للفصل فى حقوقه والتزاماته وأية تهمة جنائية توجه إليه».

وتضمنت الفقرة الثانية من المادة الحادية عشر النص على أنه لا يدان أى شخص من جراء أداء عمل أو امتناع عن أداء عمل، إلا اذا كان ذلك يعتبر جرماً وفقاً للقانون الوطنى وقت ارتكاب الجريمة.

ونصت المادة الثانية عشر على أنه: «لا يجوز تعريض أحد لتدخل تعسفى فى حياته الخاصة أو فى شئون أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته، ولكل شخص حق فى أن يحميه القانون من مثل ذلك التدخل أو تلك الحملات».

هذه مجموعة من الضوابط العالمية للبحث عن الحقيقة والوصول إلى العدالة. (للمزيد يراجع، لواء د/ عصمت عدلى، د/ طارق ابراهيم الدسوقى – حقوق الإنسان بين التشريع والتطبيق – دار الجامعة الجديدة – الإسكندرية – سنة ٢٠٠٨).

(**) تضم هذه الاتفاقية حالياً كل الدول الأعضاء فى مجلس أوروبا، والذين وصل عددهم حتى نهاية عام ١٩٩٠م ٢٤ دولة، وكان مجلس أوروبا يتكون عند تأسيسه عام ١٩٤٩ من عشر دول هى بلجيكا، الدانمارك، فرنسا، ايرلندا، ايطاليا، لوكسمبورج، هولندا، النرويج، السويد، المملكة المتحدة.

tion Europeenne Des Droits de L'homme التى تم التوقيع عليها فى ٤ نوفمبر سنة ١٩٥٠ وصارت سارية المفعول اعتباراً من ٣ ديسمبر سنة ١٩٥٣ على تأكيد احترام الحقوق والحريات التى تضمنها الاعلان العالمى لحقوق الإنسان. حيث تضمنت الاتفاقية مجموعة من النصوص التى ترسى قواعد وضوابط اقرار العدالة والبحث عن الحقيقة، فى أطار احترام حقوق الإنسان وعدم أهدار لآدميته(*).

ونستدل على هذه المؤائمة بين البحث عن الحقيقة مع مراعاة واحترام الحقوق والحريات، بما نصت عليه الفقرة الأولى من المادة الثامنة من الاتفاقية على حماية الحق فى حرمة الحياة الخاصة حيث تضمنت: «لكل شخص الحق فى احترام حياته الخاصة والعائلية ومسكنه ومراسلاته». غير أن الفقرة الثانية من ذات المادة-تعود فتورد تحفظاً بمقتضاه تسمح بإيجاد بعض القيود على هذا الحق، إذ تنص على أنه: «لا يجوز للسلطة العامة التدخل فى مباشرة هذا الحق، إلا إذا كان هذا التدخل ينص عليه القانون، ويعد اجراء ضرورياً، فى مجتمع ديمقراطى لحماية الأمن الوطنى أو الأمن العام أو الرفاهية الاقتصادية للدولة، أو لحماية النظام أو لمنع الجرائم، أو لحماية الصحة أو الآداب أو لحماية حقوق الغير وحرياتهم».

---

(*) للمزيد من التفصيل حول الاتفاقية الأوروبية لحقوق الإنسان يراجع:

- ERHUV (Ekrem): "La Convention Europeene des Droits de L'homme" Thése. Paris. 1953.
- VASAK (Karel): "La Convention Européenne des droits de L'lomme" Thése. Paris. 1963.

وقد نصت المادة الثالثة على حظر خضوع أى شخص للتعذيب أو العقوبات أو المعاملات غير الإنسانية أو الوحشية، ونصت المادة الخامسة على أن لكل فرد الحق فى الحرية وفى الأمان على شخصه. فلا يجوز حرمانه من حريته إلا فى حالات معينة ووفقاً للإجراءات المحددة فى القانون. يراجع: د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٩٦.

ويتبين من هذه الفقرة أن حماية الحياة الخاصة والعائلية والمسكن والمراسلات ليست مطلقة، بل يجوز التدخل فيها بشرطين:

أولاً، أن يكون التدخل منصوصاً عليه فى القانون.

ثانياً، أن يكون الإجراء ضرورياً فى مجتمع ديمقراطى لحماية الأمن القومى، أو ما تلى ذلك فى نص الفقرة.

كما يمكن أن يعد من الاتفاقيات التى أرست ضوابط للبحث عن الحقيقة مع مراعاة الحقوق والحريات، مشروع الميثاق العربى لحقوق الإنسان(*)، حيث نصت المادة السادسة منه على أن «للحياة الخاصة حرمة مقدسة، المساس بها جريمة، وتشمل هذه الحياة الخاصة خصوصيات الأسرة وحرمة المسكن وسرية المراسلات وغيرها من سبل المخابرة الخاصة».

ووفقاً للمادة السابعة من هذا المشروع، فإنه لا يجوز إيراد أية قيود على الوطنيين أو النظام العام أو الصحة العامة أو الأخلاق أو حقوق وحريات الآخرين وعلاوة على ما تقدم يمكن أن نلمس اهتمام الجمعية الدولية لقانون العقوبات Association internationale de droit pénal بضوابط البحث عن الحقيقة وارساء العدالة فى ضوء احترام حقوق الإنسان، من أنعقاد المؤتمر الدولى الثانى عشر الخاص بحماية حقوق الإنسان فى قانون الإجراءات الجنائية فى مدينة هامبورج بألمانيا فى الفترة من ١٦-٢٢ سبتمبر سنة ١٩٧٩ . والذى أوصى بالنسبة لحماية الحق فى حرمة الحياة الخاصة بضرورة أن ترتكز كل وسائل وإجراءات الإثبات، التى من شأنها تعطيل الحقوق الفردية والحريات على سند قانونى(**) .

---

(*) يعد هذا المشروع من الاتفاقيات الدولية ذات الطابع الإقليمى. يراجع: د/ مفيد محمود شهاب - «مشروع الميثاق العربى لحقوق الإنسان فى ضوء العهد الدولى للحقوق الاقتصادية والاجتماعية والثقافية» - بحث منشور فى حقوق الإنسان - المجلد الثانى - دار العلم للملايين - بيروت - لبنان-سنة ١٩٨٩-ص ٤١١.

(**) عقد فى القاهرة مؤتمر حماية حقوق الإنسان فى قوانين الإجراءات الجنائية فى العالم العربى فى الفترة من ١٦-٢٠ ديسمبر سنة ١٩٨٩، وقد أصدر هذا المؤتمر العديد من التوصيات منها

-/-

وفى شأن ارساء ضوابط عامة للبحث عن الحقيقة، ذهب رأى فى الفقه[1] - نؤيده - إلى أنه حرىٌ بنا أن نشير إلى أن الحقوق والحريات التى حفلت بها المواثيق الدولية وإعلانات الحقوق والمؤتمرات الدولية والاقليمية، تعتبر بمثابة ضمانات ثابتة للإنسانية غير قابلة للانتهاك Garanties humanitaires inviolables [2]، وأنه يجب على كل شخص أن يحترمها ويعمل بها وإلا عرض نفسه لاحتقار العالم وازدرائه، بل وفقد أهليته الإنسانية L'incapacité d'humanité[3] .

وفى نطاق إقامة موازنة Équilibre بين حق المجتمع فى اقرار العدالة وإنفاذ العقاب لما يرتكب من نشاط إجرامى فى نطاق المعلوماتية، والجرائم المستحدثة فى مجال التقنيات التكنولوجية الحديثة، وبين المحافظة على الحقوق والحريات فى مجال الجوانب الإجرائية - وبالأخص إجراءات التفتيش والضبط - يتحتم على مأمور الضبط القضائى الموكول له مباشرة هذه الإجراءات، احترام الضوابط العامة التى أرساتها المواثيق والتشريعات والمنظمة للحقوق والحريات، مع إعمال التقنيات الحديثة والفكر الإبداعى لتنفيذ القوانين، وضبط الجناة لاقرار حق المجتمع فى العدالة والعقاب.

**ثانياً: الضوابط العامة لتفتيش المعلوماتية:**

يمكن تقسيم الضوابط العامة لإجراء تفتيش نظم المعلوماتية إلى ضوابط موضوعية وأخرى شكلية.

---

- التوصية [١٧] التى تقرر حرمة المسكن وعدم جواز دخول المساكن بغير رضاء أصحابها إلا بموجب أمر قضائى مسبب لضبط أشياء تفيد فى كشف الحقيقة فى جريمة تستوجب عقوبة الحبس.

- كما عقدت الجمعية المصرية للقانون الجنائى مؤتمرها الثانى عن حماية الإنسان فى الإجراءات الجنائية فى مصر وفرنسا والولايات المتحدة الأمريكية، فى الإسكندرية من ١٢/٩ إبريل ١٩٨٨.

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١٠.

(2) RAVIER (Paul): "La Reherche de la vérité judiciaire et l'audition interrogatoire du suspect" thése Paris II, 1973, p. 50

- Ibid., p. 46.

(٣) صاحب هذا التعبير المفكر الفرنسى جان جاك روسو.

• **الضوابط الموضوعية لتفتيش نظم المعلوماتية:**

أجملت محكمة النقض في أحد أحكامها مبررات القيام بالتفتيش، حيث تعد هذه المبررات من الضوابط الموضوعية التي يتم تنفيذ إجراء التفتيش في سياقها، وقد قضت محكمة النقض بأن[1]:

«الأصل في القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة – جناية أو جنحة – واقعة بالفعل وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفي للتصدي لحرمة مسكنه أو لحرمته الشخصية».

وبناء على ذلك فإن سبب التفتيش – في الجرائم التقليدية – بوصفه اجراء من اجراءات التحقيق هو[2]:

– وقوع جناية أو جنحة.

– اتهام شخص أو أشخاص معينين بارتكابها أو المشاركة فيها.

– توافر امارات قوية أو قرائن على وجود أشياء تفيد في كشف الحقيقة لدى المتهم أو غيره.

وفي مجال المعلوماتية لابد أن نكون بصدد جريمة معلوماتية واقعة بالفعل (سواء كانت جناية أو جنحة)، واتهام شخص أو أشخاص معينين بارتكاب هذه الجريمة أو المشاركة فيها، وتوافر امارات قوية أو قرائن على وجود أجهزة معلوماتية تفيد في كشف الحقيقة لدى المتهم أو غيره.

**أ- ضبط جريمة معلوماتية - واقعة بالفعل - جناية أو جنحة:**

أوضحنا سابقاً أنه لا يوجد تعريف محدد ومتفق عليه بين الفقهاء حول

---

(١) نقض ١٦ أكتوبر سنة ١٩٦٧ – مجموعة أحكام النقض – س ١٨ – رقم ١٩٥ – ص ٩٦٥.

(٢) د/ هلالي عبد اللاه أحمد – المرجع السابق – ص ١٠٤.

مفهوم الجريمة العلوماتية Le délit informatique . إذ مذهم المضيق لهذا المفهوم ومذهم الموسع[1].

ويلاحظ – كما ذهب رأى[2] فى ذلك نتفق معه – أن التعريفات التى تناولتها الآراء بشأن الوقوف على السلوك الإجرامى للمعلوماتية، قد حاولت أن تعرف الجرائم الواقعة – المرتكبة – فى مجال المعلوماتية، لكنها أخفقت حين أهملت الجرائم التى ترتكب بحق الأشخاص من خلال استخدام وسائط المعلوماتية، وبالخصوص الجرائم المرتكبة باستخدام الإنترنت وهى مشكلة الساعة. حيث لم تأخذ حظها الكافى فى مجال القانون الجنائى. إذ لم تتناول هذه التعريفات الجرائم الحديثة كالقذف والتهديد بالقتل، والجرائم المنظمة وجرائم الجاسوسية، والتعدى على أمن الدولة ... وغيرها من الجرائم التى تندرج ضمن التعريفات التى ذكرت.

وقد عرض ذات الرأي لتعريف للجريمة المعلوماتية بأنه[3]:

«سلوك إجرامى، إيجابى أو سلبى من شأنه الاعتداء بأى صورة من الصور، على الشخص المعنوى أو الاعتبارى بفعل يلحق به ضرراً أو يعرضه لضرر محتمل، أو يحصل على كسب بدون وجه حق كنتيجة لهذا الفعل، أو من شأنه الاعتداء بأى صورة من الصور على المعلومات أو البيانات المخزنة داخل الحاسب، أو داخل وسائط أخرى يتم تخزين المعلومات فيها من خلاله، على نحو يلحق ضرراً فعلياً أو مفترضاً بالجهة التى تم تخزين المعلومات لمصلحتها».

**- تقييم التعريف:**

أغفل التعريف السابق جانب هام، وهو المتعلق بالحماية القانونية التى تقرر

---

(1) راجع ما تقدم فى الدراسة ص .

(2) د/ محمود عبد الرحيم الديب – مرجع سابق – ص ٤٠٧ .

(3) المرجع ذاته.

عقوبة على السلوك الإجرامى المرتكب، وتحافظ على الشرعية الجنائية "Nulum crimena mulla pocna sinclege" والتى تعنى أنه لا جـريمـة ولا عـقـوبة إلا بنص.

إذا أنه لا يمكن أن يوجه أى أتهام ضد شخص لارتكابه فعلاً معيناً، ما لم يكن منصوصاً على تجريم هذا الفعل فى القانون، كما لا يمكن تطبيق عقوبة ما لم تكن محددة سلفاً(١).

كما أسهب التعريف فى وصف صور الإعتداء. واحتمالات الضرر، وأشكال المعلومات، بشكل زاد من الأطار العام للتعريف.

ونخلص من ذلك إلى أن جرائم المعلوماتية من الصعب الحسم فى تحديد تعريفها – ان لم يكن غير ممكن – حيث تتسم العناصر المكونة لهذه الجرائم بالتجدد والتطور التقنى، حسبما يلاحق بالمعلوماتية وانظمتها ومكوناتها من تطور مستمر ورقى تكنولوجى فى أزدياد. إذ تستحدث العقول البشرية كل يوم أنماط جديدة من الجرائم المرتكبة، والعابثة فى مجال المعلوماتية لا يمكن توقعها مسبقاً.

**- أهمية توصيف السلوك الضار بالمعلوماتية بالجريمة:**

مؤدى أن يتضمن تعريف الجريمة المعلوماتية النص على الحماية القانونية، المحافظة على الشرعية الجنائية، وهذه السمة تعنى أن يحدد قانون العقوبات مقدماً الأفعال التى تعتبر جرائم معلوماتية، وينص على العقوبات المقررة لها. وهذا ما أقدمت عليه بعض الدول، ففى المملكة المتحدة مثلاً صدر قانون إساءة استخدام الحاسب Computer Misuse act فى ٢٩ يونيه سنة ١٩٩٠ وطبق

---

(١) لمراجعة المزيد من التفصيل حول مبدأ الشرعية الجنائية أنظر:

- BENLATRCHE (Abd el Wahab): "Le Pricipe de la légalité Criminlle. Etude de droit comparé:. Thése. Poitiers, 1981.

اعتباراً من ٢٩ أغسطس ١٩٩٠[١]. وفى الولايات المتحدة الأمريكية صدر قانون الاحتيال وإساءة استخدام الحاسب سنة ١٩٨٦، والذى طبق على المستوى الفيدرالى[٢]، بالإضافة إلى قوانين صدرت فى بعض الولايات مثل قانون ولاية تكساس الصادر فى أول سبتمبر سنة ١٩٨٥ بشأن الدخول غير المشروع على نظام الحاسب. وفى فرنسا صدر القانون رقم ٨٨/١٩ فى ٥ يناير سنة ١٩٩٨، والذى أطلق عليه قانون الغش المعلوماتى La fraude informatique[٣]، والذى تم تعديله مع صدور قانون العقوبات الفرنسى الجديد الذى بدأ العمل به اعتباراً من أول مارس سنة ١٩٩٤[٤]. وفى الدنمارك صدر قانون جرائم الحاسب فى ٦ يونيه سنة ١٩٨٥.

وفى مصر أدرج المشرّع مصنفات الحاسب الآلى من برامج وقواعد بيانات وما يماثلها من مصنفات تحدد بقرار من وزير الثقافة(*)، ضمن المصنفات المشمولة بحماية حق المؤلف، المنصوص عليها فى المادة الثانية بمقتضى القانون رقم ٣٨ لسنة ١٩٩٢م، الخاص بتعديل بعض أحكام قانون حق المؤلف رقم ٣٤٥ لسنة ١٩٥٤ والمعدل بالقانون رقم ٢٩ لسنة ١٩٩٤(**).

---

(1) FERBRACHE (David): op. cit., p. 233.

(2) JACKSON (K.M) & HRUSKA (J.): "Computer security. Reference book. Editor Donn B.". Parker, 1992, p. 401.

(3) CHAMAUX (Fra .nçais): "La loi sur la fraude informatique. de nouvelles incriminations: J.C.P. 1988-1-3321.

(٤) راجع ما سبق فى الدراسة ص٣٦٨. بشأن التشريعات المواجهه للإجرام المعلوماتى.

(*) تضمنت المادة الثانية من قرار وزير الثقافة رقم ٨٢ لسنة ١٩٩٣ فى شأن تنفيذ قانون حماية المؤلف فيما يتعلق بمصنفات الحاسب الآلى، معانى بعض العبارات الواردة فى القرار من تعريف للحاسب الآلى وبرنامج الحاسب وقاعدة البيانات وقد ادرجت فى (الوقائع المصرية العدد رقم ١٠٤ الصادر فى ١٩٩٣/٥/٩).

(**) شدد هذا التعديل عقوبة الاعتداء على حقوق التأليف، لتصبح الحبس والغرامة التى لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه، أو إحدى هاتين العقوبتين، بدلاً من عقوبة الغرامة التى تتراوح ما بين ١٠ و ١٠٠ جنيه.

-/-

كما استحدث المشرع المصرى قانوناً لحماية البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين، والتى تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الخاصة بمصلحة الأحوال المدنية بوزارة الداخلية، وهو القانون رقم ١٤٣ لسنة ١٩٩٤ فى شأن الأحوال المدنية الصادر فى ٩ يونية ١٩٩٤(*).

وقد قصر المشرع المصرى حمايته الجنائية على مجالين من مجالات الحاسب الآلي، أولهما: البرامج وقواعد البيانات. وهذه اعتبرها ضمن المصنفات المشمولة بحماية حق المؤلف.

والثاني: البيانات الفردية التى تقتضى إجراء احصاء للسكان. وكذلك البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين.

وهذه نص على العقوبات التي ينبغي تطبيقها فى حالة الاعتداء عليها، أما بقيه الجرائم المعلوماتية التى تمثل اعتداء على نظم المعلوماتية، وسواءاً كان الحاسب الآلى موضوعاً للجريمة أو أداة لارتكابها، فلا تشملها الحماية الجنائية.

-- ويتعرض للعقوبة المنصوص عليها من يعتدى على حق من حقوق المؤلف المنصوص عليها فى المواد ٥، ٦، ٧ من القانون، وكل من أدخل فى مصر بقصد الاستغلال دون إذن المؤلف مصنفاً منشوراً فى الخارج مما تشمله الحماية التى تفرضها أحكام هذا القانون. (راجع ما سبق من الدراسة ص ).

ويجوز للمحكمة عند الحكم بالإدانة ان تقضى بغلق المنشأة التى استغلها المقلدون أو شركائهم فى ارتكاب أحد الافعال المشار إليها مدة لا تزيد على ستة أشهر. (راجع أحكام المادة ٤٧ المعدلة بالقانون رقم ٣٨ لسنة ١٩٩٢).

(*) نصت المادة الثالثة عشر من هذا القانون على ما يأتى:

«تعتبر البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين، والتى تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين الملحقة بسرية، ولا يجوز الاطلاع عليها أو الحصول على بياناتها إلا فى الأحوال التى نص عليها القانون ووفقاً لأحكامه.

وتعتبر البيانات أو المعلومات أو الإحصائيات المجمعة التى تشتمل عليها السجلات أو الدفاتر أو الحاسبات الآلية أو وسائط التخزين سرا قومياً، ولا يجوز الاطلاع عليها أو نشرها إلا لمصلحة قومية أو علمية، وبإذن كتابى من مدير مصلحة الأحوال المدنية أو ممن ينيبه، وفقاً للأوضاع والشروط التى يحددها القانون واللائحة التنفيذية.

وبالنسبة لمجالات نظم المعلوماتية المشمولة بالحماية الجنائية فى مصر، فمن الأهمية أن نشير إلى أن إجراء التفتيش بالنسبة لها لا يتخذ إلا بصدد جريمة قد ارتكبت بالفعل. فلا يصح القيام به لضبط جريمة مستقبلة(1)، ولو قامت التحريات والدلائل الجدية على أنها ستقع بالفعل(2).

فلو فرض مثلا أن التحريات أثبتت أن شخصاً معيناً سوف يتجر فى برامج نظم معلومات – مقلدة أو منسوخة – مما يعد اعتداء على حق المؤلف، وأنه سيتسلم كمية من هذه البرامج فى يوم معين، فصدر أمر من النيابة العامة لضبطه وتفتيش ما يحوزه عند تسلمه هذه البرامج، فان هذا الأمر يقع باطلاً لأنه صدر من أجل جريمة مستقبلة، وبالتالى لا تتحرك به الدعوى(3). لكن إذا كان مأمور الضبط القضائى لم يقم بتفتيش ما يحوزه المتهم المعلوماتى، إلا بعد أن شاهده وهو يتسلم هذه البرامج المنسوخه، فإنه يكون قد شاهد الجريمة فى حالة تلبس مما يبرر له تفتيش ما يحوزه بناء على هذه الحالة وحدها.

---

(1) نقض ١٨ ديسمبر سنة ١٩٨٦ – مجموعة أحكام النقض – س ٥٦ ق – رقم ٢٠٦ – ص ١٠٨٥، نقض ١٦ يناير سنة ١٩٨٦ – مجموعة أحكام النقض – ص ٥٥ ق – رقم ٢١ – ص ٩٤، نقض ١٤ يناير سنة ١٩٨٦ – مجموعة أحكام النقض – س ٥٥ ق – رقم ١٤ – ص ٦٤.

(2) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١١٤.

(3) الطعن رقم ١٥٣٨ لسنة ٤٤ قضائية – جلسة ١٩٧٤/١٢/٢٢ – س ٢٥ – ص ٨٧٦ – أحكام محكمة النقض.

ومفاده.. أن صدور الإذن بضبط وتفتيش المتهم – إستناداً إلى ما دلت عليه التحريات من اتجاره بالمخدرات وترويجها. النعى على الإذن بأنه صدر لضبط جريمة مستقبله – غير صحيح.

مضمون الحكم: إذا كان الحكم المطعون فيه قد أثبت أن الشاهد استصدر إذن النيابة بالتفتيش بعد أن دلت تحرياته على أن الطاعن يتجر فى المخدرات ويقوم بترويجها، ويحتفظ بإجزاء منها بمسكنه، فإن مفهوم ذلك أن الأمر قد صدر لضبط جريمة تحقق وقوعها من مقارفها لا لضبط جريمة مستقبلة أو محتملة، وإذ انتهى الحكم إلى أن الأذن قد صدر لضبط جريمة واقعة بالفعل وترجحت نسبتها إلى المأذون بتفتيشه وليس عن جريمة مستقبلة، فأنه يكون قد أصاب صحيح القانون.

كذلك اذا ثبت من تحريات الشرطة أن المتهم المعلوماتي كان يحتفظ بهذه البرامج المقلدة بين امتعته. وصدر الإذن بتفتيش ما يحوزه أو يحرزه حال نقل هذه الأمتعة، فإن الأمر يكون قد صدر لضبط جريمة معلوماتية تحقق وقوعها من مقارفها، لا لضبط جريمة مستقبلة(١).

كما أنه لا يكفى مجرد وقوع جريمة معلوماتية للقول بجواز إجراء التفتيش، بل لابد أن تكون مما يعتبرها القانون جناية أو جنحة(*)، وبالنسبة للجنحة فإن القانون لم يشترط أن تكون الجنحة معاقباً عليها بالحبس، فيصح أن تكون عقوبتها الغرامة. بيد أن المشرع أشترط أن تكون الجنحة معاقباً عليها بالحبس مدة تزيد على ثلاثة أشهر، فى الأمر بالضبط إذا تعلق برسائل أو بمراقبة المحادثات السلكية أو اللاسلكية أو إجراء تسجيلات (م ٩٥ أ-ج)، ويمكن أن يتعلق ذلك ببعض نظم المعلوماتية.

وفى كلمة جامعة(**)، نخلص إلى القول أن الشرط الأول من شروط سبب التفتيش نظم المعلوماتية، هو أن نكون بصدد جريمة معلوماتية واقعة بالفعل سواء كانت جناية أو جنحة لا يتوافر إلا بالنسبة لمجالين من مجالات المعلوماتية، أضفى عليهما المشرع الجنائى المصرى حمايته هما:

---

(١) الطعن رقم ٦٤٣ لسنة ٤٤ ق – أحكام محكمة النقض – جلسة ٢٣ يونيه سنة ١٩٧٤ – س ٢٥ – ص ٦٢١، وأيضاً الطعن رقم ٥١٢ لسنة ٤١ ق – جلسة ١٧ أبريل سنة ١٩٧٦ – مجموعة القواعد القانونية (فنى) – س ٢٧ – ص ٧٦٣. وقد تضمن أن الأمر بالتفتيش إنما صدر لضبط المتهم حال نقله للمخدر بالسيارة باعتبار أن هذا النقل مظهراً لنشاطه فى الاتجار بالمخدرات، بما مفهومه أن الأمر صدر لضبط جريمة تحقق وقوعها من مقارفها لا لضبط جريمة مستقبلة أو محتملة، ومن ثم فان الحكم المطعون فيه اذ قضى بأن اذن التفتيش صدر عن جريمة لم ثبت وقوعها يكون قد أخطأ فى تطبيق القانون، بما يستوجب نقضه.

(*) وبالتالى تستبعد المخالفات. ذلك لأن المخالفات من ضآلة شأنها بحيث لا يتوافر لها من التفتيش، والعبرة بوصف التهمة هى بما يجرى التحقيق بشأنه، دون ما يسفر عنه فى نهايته.

(**) كما ذهب فى ذلك د/ هلالى عبد اللاه أحمد فى مرجعه السابق – ص ١١٥.

١- البرامج وقواعد البيانات التى اعتبرها ضمن المصنفات المشمولة بحماية حق المؤلف.

٢- البيانات الفردية التى تقتضى إجراء إحصاء للسكان، وكذلك البيانات والمعلومات المتعلقة بالأحوال المدنية للمواطنين.

ونضيف إلى ما سبق مجال أخر جديد أستحدثه المشرع بأصداره القانون رقم ١٥ لسنة ٢٠٠٥ بشأن تنظيم التوقيع الالكترونى، وهو مجال:

- اصدار شهادات التصديق الالكترونى، أو أتلاف أو عيب توقيعاً أو وسيطاً أو محرراً إلكترونياً، أو تزوير محرراً إلكترونياً بطريق الاصطناع أو التعديل أو التحوير أو بأى طريق آخر.
- أو استعمال توقيعاً أو وسيطاً أو محرراً إلكترونياً معيباً أو مزوراً مع العلم بذلك.
- الحصول بغير حق على توقيع أو وسيط أو محرر الكترونى، أو اختراق هذا الوسيط أو اعتراضه أو تعطله عن أداء وظيفته.

وقد تضمن هذا المجال المادة ٢٣ من القانون ١٥ لسنة ٢٠٠٥ بشأن تنظيم التوقيع الالكترونى، كما تضمنت ذات المادة فى فقرة (د) مجالا أخر مستحدثاً هو:

- مخالفة أيا من أحكام المادتين (١٩)، (٢١) من هذا القانون(*).

---

(*) تنص المادة (١٩) على أنه: (لا يجوز مزاولة نشاط إصدر شهادات التصديق الإلكترونى إلا بترخيص من الهيئة.........)

والمقصود بالهيئة: هيئة تنمية صناعة تكنولوجيا المعلومات، التى نصت المادة الثانية من القانون ١٥ لسنة ٢٠٠٥ على أنشاءها هيئة عامة.

وتنص المادة (٢١) على أن: (بيانات التوقيع الإلكترونى والوسائط الإلكترونية والمعلوماتية التى تقدم إلى الجهة المرخص لها بإصدار شهادات التصديق الإلكترونى سرية، ولا يجوز لمن قدمت إليه أو أتصل بها بحكم عمله إفشاؤها للغير أو استخدامها فى غير الغرض الذى قدمت من أجله).

ب- اتهام شخص أو أشخاص معينين بارتكاب الجريمة المعلوماتية أو المشاركة فيها:

ينبغى أن تتوافر فى حق الشخص المراد تفتيشه - شخصه أو مسكنه - دلائل كافية تدعو للاعتقاد بأنه قد ساهم فى ارتكاب الجريمة المعلوماتية، سواء بوصفه فاعلاً أو شريكاً مما يستوجب أتهامه بها. بحيث إذا لم تتوافر هذه الدلائل، يكون على قاضى التحقيق أن يصدر أمراً بأن لا وجه لإقامة الدعوى(١).

ونفس الفكرة يمكن تأكيدها فى القانون الأمريكى، الذى يوجب انهاء الإجراءات إذا وجد قاضى التحقيق Grand Jury فى نهاية التحقيق الابتدائى عدم وجود سبب معقول Probable cause يدعو للاعتقاد بأن الشخص قد ارتكب الجريمة(٢).

وهذا أيضاً ما يقرره قانون الإجراءات الجنائية الفرنسى فى المادة (١٧٧) التى توجب على قاضى التحقيق أن يأمر بأن لا وجه لإقامة الدعوى إذا لم يجد إثباتات كافية Charges suffisantes ضد المتهم(٣).

وفى مجال المعلوماتية.. يمكن القول بأن تعبير الدلائل الكافية يقصد به مجموعة من المظاهر أو الأمارات المعينة التى تنهض على السياق العقلى والمنطقى لملابسات الواقعة، وكذلك على خبرة وحرفية القائم بالتفتيش، والتى

---

(١) هذا ما تؤكده المادة ١٥٤ من قانون الإجراءات الجنائية المصرى بقولها: «إذا رأى قاضى التحقيق.... إن الأدلة على المتهم غير كافية يصدر أمراً بأن لا وجه لإقامة الدعوى».

(2) KEBEICH (M.): "L'inculpation, étude du droit francais, essai de rapprochement avec Le droit égyptien et Le droit des Etats-unis D'Amerique: thése Poitiers, 1984.

(3) MERLE (R.): "L'inculpation en problemés contemparains de procédure Pénale: Mélanges HUGUENEY, Sirey, Paris, 1964.

مشار إليه لدى: د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١١٥ - هامش ١.

تؤيد نسبة الجريمة المعلوماتية إلى شخص معين، سواء بوصفه فاعلاً أو شريكاً(*) .

**جـ- توافر أمارات قوية أو قرائن تفيد في كشف الحقيقة:**

لا يكفى لحث سلطة التحقيق إلى إصدار قرارها بالتفتيش ومباشرته مجرد وقوع جناية أو جنحة، واتهام شخص معين بارتكابها أو المشاركة فيها.

بل يجب أن تتوافر أمارات قوية أو قرائن على وجود أشياء أو أجهزة أو معدات معلوماتية تفيد فى كشف الحقيقة لدى المتهم المعلوماتى أو غيره. ومعنى ذلك أنه يستوى أن تكون هذه الأشياء أو الأجهزة المعوماتية فى حيازة الشخص أو فى منزله أو أن يكون هذا الشخص متهماً أو ليس كذلك. كل ما هنالك أنه إذا كان الشخص غير متهم فإن تفتيشه هو أو منزله يخضع لأحكام خاصة(1) .

وهكذا، فالتفتيش لا يجرى إلا إذا توافرت لدى المحقق أسباب كافية على أنه يوجد فى المكان أو لدى الشخص المراد تفتيشه، أدوات استعملت فى الجريمة المعلوماتية أو أشياء متحصلة منها أو أية أشياء أو مستندات اليكترونية يحتمل أن يكون لها فائدة فى استجلاء الحقيقة لدى المتهم المعلوماتى أو غيره(**) .

وهذا يتطلب أن يسبق التفتيش تحريات جدية تسوغ الأمر به، بحيث إذا تم التفتيش دون أن تسبقه تحريات جدية، تنبئ عن وجود دلائل قوية على حيازة

---

(*) يراجع ما سبق فى ا لدراسة ص ، بشأن المشروعية والدلائل الكافية.

(1) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢٢ .

(**) «من المقرر أن كل ما يشترط لصحة التفتيش الذى تجريه النيابة أو تأذن فى إجرائه فى مسكن المتهم أو ما يتصل بشخصه هو أن يكون رجل الضبط القضائى قد علم من تحرياته واستدلالاته أن جريمة معينة – جناية أو جنحة – قد وقعت من شخص معين أو أن تكون هناك من الدلائل والأمارات الكافية والشبهات المقبولة ضد هذا الشخص بقدر يبرر تعرض التفتيش لحرية أو لحرمة مسكنه، فى سبيل كشف اتصاله بالجريمة المعلوماتية. (نقض ٢٦ يناير ١٩٨١ – مجموعة أحكام محكمة النقض – ص ٥٠ ق – رقم ١٢ – ص ٧٩) .

ما تم تفتيشه لأشياء أو أجهزة معلوماتية تفيد فى كشف الحقيقة، وأسفر هذا التفتيش عن كشف جريمة، فإنه لا يعتد بهذا التفتيش ولا بنتائجه(*).

وتقدير جدية التحريات وكفايتها لإصدار الإذن بالتفتيش هو من المسائل الموضوعية التى يوكل الأمر فيها إلى سلطة التحقيق، تحت إشراف محكمة الموضوع(1). ومن ثم فإذا أراد المتهم أن يدفع ببطلان التفتيش لعدم جدية

---

(*) وتطبيقاً لذلك قضت محكمة النقض بأنه إذا:

«كان الثابت بمحضر التحريات الذى صدر الإذن مستنداً إليه أن ... رئيس وحدة مباحث مركز شربين هو الذى قام بالتحريات والمراقبة للمتهم حتى تأكد أنه يحوز المخدر ويتجر فيه بينما أثبت هو نفسه بمحضر ضبط الواقعة أنه انتقل وبرفقته قوة من الشرطة السريين لتنفيذ الإذن.. وخلف مقهى بشارع الجيش أمام سور مستشفى شربين العام من الناحية الشرقية وجد شخصاً جالساً بمفرده وعندما سأله عن اسمه تبين له أنه الشخص الذى استصدر إذن النيابة بضبطه وتفتيشه وقد وردد ذلك وأكده فى أقواله بتحقيق النيابة وأضاف أن التحريات التى أجراها مصدرها سرى وأنه لا يعرف شخص المتهم الأمر الذى يدحض ما ذكره بمحضر التحريات الذى صدر الإذن استناداً إلى ما جاء به من أن التحريات التى أجراها ومراقبته المستمرة للمتهم أكدت له حيازة المتهم للمخدر وتضحى هذه التحريات مجرد بلاغ تلقاه من مرشد سرى أو شخص ما بأن المتهم يحوز مخدراً بقصد الاتجار وهو ما لا يصلح بحال لإصدار إذن التفتيش لانعدام التحريات الجدية ومن ثم يكون الدفع ببطلان الإذن بضبط المتهم وتفتيشه قد استقام على سند صحيح من الواقع والقانون ويكون الإذن وما تلاه وترتب عليه باطلاً. (نقض ١٦ يناير سنة ١٩٨٠ مجموعة أحكام النقض س ٤٩ رقم ١٧ ص ٨٥).

(1) نقض ٢ نوفمبر سنة ١٩٨٦ مجموعة أحكام النقض س ٥٦ رقم ١٧٧ ص ٩٣٢، نقض ٤ يونيه ١٩٨٦ مجموعة أحكام النقض س ٥٦ رقم ١٢٠ ص ٦٣٠، نقض ٢٣ أبريل ١٩٨٦ مجموعة أحكام النقض س ٥٦ رقم ١٠١ ص ٥٠٨، نقض ١٤ يناير سنة ١٩٨٦ مجموعة أحكام النقض س ٥٥ رقم ١٤ ص ٦٤، نقض ٢٦ يناير سنة ١٩٨١ مجموعة أحكام النقض س ٥٠ رقم ١٢ ص ٧٩، نقض ١٦ يناير سنة ١٩٨٠ مجموعة أحكام النقض س ٤٩ رقم ١٧ ص ٨٥، نقض ٢٤ أبريل سنة ١٩٨٠ مجموعة أحكام النقض س ٤٩ رقم ١٠٥ ص ٥٥٢ نقض ٢٤ نوفمبر سنة ١٩٨٠ مجموعة أحكام محكمة النقض س ٥٠ رقم ١٩٩ ص ١٠٢٩، نقض ١٧ مايو سنة ١٩٧٩ - مجموعة أحكام النقض س ٤٩ رقم ١٢٥ ص ٥٨٨، نقض ١٩ أبريل سنة ١٩٧٩ مجموعة أحكام النقض س ٤٨ رقم ١٠٣ ص ٤٩٠، نقض ١١ يناير سنة ١٩٧٩ مجموعة أحكام النقض س ٤٨ رقم ٨ ص ٥٤.

التحريات التى سبقته كان عليه أن يتقدم بدفعه إلى محكمة الموضوع، إذ لا تجوز إثارة الجدل بشأنه لدى محكمة النقض(*).

وفى هذه الحالة على محكمة الموضوع أن تعرض له وتقول كلمتها فيه بأسباب سائغة(1). وفى هذا النطاق يخضع قضاؤها لرقابة محكمة النقض فى إطار النظرية العامة التى تراقب فيها هذه الأخيرة التدليل فى الأحكام المطعون فيها(**).

---

(*) وفى ذلك تقول محكمة النقض إنه: «من المقرر أن - تقدير جدية التحريات وكفايتها لإصدر الإذن بالتفتيش هو من المسائل الموضوعية التى يوكل الأمر فيها إلى سلطة التحقيق تحت إشراف محكمة الموضوع. فإذا كانت المحكمة قد اقتنعت بجدية الاستدلالات التى بنى عليها إذن التفتيش وكفايتها لتسويغ إجرائه كما هو الشأن في الدعوى المطروحة، فلا يجوز المجادلة فى ذلك أمام محكمة النقض (نقض ٢٤ نوفمبر سنة ١٩٨٠ - مجموعة أحكام النقض - س ٥٠ - رقم ١٩٩ - ص ١٠٢٩).

(1) نقض ٢٠ أكتوبر سنة ١٩٨١ مجموعة أحكام النقض رقم ١٢٨ ص ٧٢٨.

(**) وفى ذلك تقول محكمة النقض إن: «تقدير جدية التحريات وكفايتها لتسويغ إصدار الإذن بالتفتيش وإن كان موكولاً إلى سلطة التحقيق التى أصدرته تحت رقابة محكمة الموضوع، إلا أنه إذا كان المتهم قد دفع ببطلان هذا الإجراء، فإنه يتعين على المحكمة ان تعرض لهذا الدفع الجوهرى، وأن ترد عليه بالقبول أو الرفض وذلك بأسباب سائغة، فإذا كان الحكم المعطون فيه قد عول فى رفض الدفع ببطلان إذن التفتيش بعدم جدية التحريات على القول بأن ضبط المخدر فى حيازة الطاعن دليل على جدية تحريات الشرطة، فإن ذلك لا يصلح رداً على هذا الدفع ذلك بأن ضبط المخدر هو عنصر جديد فى الدعوى لاحق على تحريات الشرطة وعلى إصدار الإذن بالتفتيش بل إنه هو المقصود بذاته بإجراء التفتيش. فلا يصح أن يتخذ منه دليلاً على جدية التحريات السابقة عليه، أن شرط صحة إصدار الإذن أن يكون مسبوقاً بتحريات جدية يرجح معها نسبة الجريمة إلى المأذون بتفتيشه، بما كان يقتضى من المحكمة - حتى يستقيم الدفع - أن تبدى رأيها فى عناصر التحريات السابقة على الإذن دون غيرها من العناصر اللاحقة عليه، وأن تقول كلمتها فى كفايتها أو عدم كفايتها لتسويغ إصدار الإذن من سلطة التحقيق. أما وهى لم تفعل، فان حكمها يكون معيباً بالقصور والفساد فى الاستدلال. (نقض ٦ فبراير سنة ١٩٧٢ مجموعة أحكام النقض س ٤٢ رقم ٣٤ ص ١٢٦).

كما قالت فى حكم أحدث إنه: «لما كان الأصل فى القانون أن الإذن بالتفتيش هو إجراء من إجراءات التحقيق لا يصح إصداره إلا لضبط جريمة «جناية أو جنحة» واقعة بالفعل، وترجحت نسبتها إلى متهم معين، وأن هناك من الدلائل ما يكفى للتصدى لحرمة مسكنه و لحريته الشخصية، وكان من المقرر أن تقدير جدية التحريات وكفايتها لتسويغ إصدار الإذن بالتفتيش وإن

-/-

**- أهمية علم مأمور الضبط القضائي بتقنيات نظم المعلوماتية لتقدير صحة التحريات التي يجريها في نطاق الجريمة المعلوماتية:**

تعرض الفقه والقضاء فى مصر لتقدير صحة التحريات فى الجرائم التقليدية، ولم يتم تناولها فى الجرائم المستحدثه - الجرائم الافتراضية - والتى منها الجريمة المعلوماتية، فهل يشترط علم ومعرفة مأمور الضبط القضائى بتقنيات نظم المعلومات كدليل - سند - على صحة التحريات التى قام بها وهو فى سبيله لتسطير محضر يذيله بطلب ضبط وتفتيش المتهم المعلوماتى؟

بداية: التحرى فى الأمور - أصطلاحاً - يعنى قصدُ أفضلها، وتحرى الشئ قصده وتوخاه وإجتهد فى طلبه ودقق فيه، ويقال تحرى عنه(*). والتحرى فى الأشياء ونحوها: طلب ما هو (أحرى) بالاستعمال فى غالب الظن أى أجدر وأخلق. واشتقاقه من قولك، هو (حرِى) أن يفعل كذا، أى جدير وخليق، وفلان تيحرى) كذا أى يتوخاه ويقصده، وقوله تعالى: (فأولئك تحروا رشداً) أى توخوا وعمدوا(١).

---

كان موكولاً إلى سلطة التحقيق التي أصدرته تحت رقابة محكمة الموضوع، إلا إنه إذا كان المتهم قد دفع ببطلان هذا الإجراء، فأنه يتعين على المحكمة أن تتعرض لهذا الدفع الجوهرى، وأن تقول كلمتها فيه بأسباب كافية وسائغة، وإذا كان الحكم قد اكتفى فى الرد على الدفع ببطلان إذن التفتيش بقوله «إن أوراق الدعوى خلت من أى دليل على اصطحاب الضابط المرشد السرى أثناء التفتيش». وهى عبارة قاصرة لا يستطاع معها الوقوف على مسوغات ما قضى به الحكم فى هذا الشأن. إذ لم تبد المحكمة رأيها فى عناصر التحريات السابقة على الإذن بالتفتيش أو تقل كلمتها فى كفايتها لتسويغ إصدار الإذن من سلطة التحقيق. لما كان ما تقدم، فإن الحكم يكون معيباً بالقصور والفساد في الاستدلالات - (نقض ١٢ فبراير ١٩٧٩ مجموعة أحكام النقض س ٤٨ رقم ٥٢ ص ٢٦٥).

(*) ويقال حرى الشيء - إتجه نحوه - كما يقال، حرى أن يكون ذلك: أى عسى، أما الأحرى: الأفضل والأجدر - المعجم الوجيز - صادر عن مجمع اللغة العربية - طبعة ١٤١٠هـ - ١٩٩٠م - ص ١٤٧.

(١) مختار الصحاح - للشيخ الإمام (محمدين أبى بكر بن عبد القادر الرازى) - مكتبة لبنان - لبنان - طبعة سنة ١٩٨٦ - باب الحاء - ص ٥٦.

ويقصد بالتحرى فى مجال الضبط القضائى: البحث عن الجرائم المرتكبة والتحقيق من صحة الوقائع المبلغة لمأمور الضبط القضائى. وجمع كافة القرائن التى تفيد فى حصول الواقعة أو نفى وقوعها(١).

والتحقيق يقصد به الأثبات – يقال حّقق الأمر أثبته وصدقه. و (الحق) ضد الباطل وحقق الشيء والأمر: أحكمه، و (تحقق) عنده الخبر صح، وتحقق قوله وظنه أى صدقه(*).

وقد أثبتت التجربة العملية فى المجال الضبطى أن مباشرة التحريات والاستخبارات، هى من أهم وأدق المهام الملقاه على عاتق الجهاز الشرطى، باعتبار أن من واجبه – كما نص القانون – على اختلاف تخصصاته فى أى مجتمع من المجتمعات القيام بالكشف عن الجرائم المرتكبة فضلا عن عمليات المكافحة ذاتها ومنع الجرائم قبل وقوعها. (م ٣ من القانون ١٠٩ لسنة ١٩٧١ بشأن هيئة الشرطة).

ولامراء فى أن عملية الكشف عن الجريمة بصفة عامة Crime Détection بما تتضمنه عن مرحلتى البحث Investigation والتحرى، وبالتالى التعرف Identification، أضحت الأن بالدرجة الأولى تركز على الجهود التى تبذل من العمل المنظم والجهد المضنى Hard solid work(٢).

• **الوضع القانوني للمسألة:**

لم يتعرض المشرع الإجرائى الا تعرضاً ضمنياً طفيفاً للتحريات (م ٢١ أ–جـ)، وهكذا كانت التحريات وكيفية القيام بها من الأمور التى لم ينظمها

(١) نقض ٣ يناير سنة ١٩٦٦ – أحكام محكمة النقض – س ١٧ ق – رقم ٢ – ص ٥.

(*) والحاقة: القيامة سميت بذلك لأن فيها حواق الأمور. (مختار الصحاح – المرجع السابق – باب الحاء – ص ٦٢.

(٢) لواء د/ قدرى عبد الفتاح الشهاوى – مناط التحريات (الاستدلالات والإستخبارات) – منشأة المعارف – الاسكندرية – سنة ١٩٩٨ – ص ١١٧.

المشرع، وبالتالى أضحت من الأمور التى تحتاج إلى وضع ضوابط تُستمد منها، خاصة أن القانون لا يوجب حتماً أن يتولى مأمور الضبط القضائى بنفسه التحريات التى يؤسس عليها الطلب بتفتيش الشخص، أو أن يكون على معرفة شخصية سابقة به(*).

ونظراً لأن بعضاً من إجراءات التحقيق لا يمكن مباشرتها فى حالات معينة إلا إذا توافرت تحريات جدية أمام سلطة التحقيق حتى تأذن بها. كما هو الحال فى مباشرة التفتيش بمعرفة مأمور الضبط القضائى بناء على إذن من النيابة بمباشرة هذا الإجراء، ومستندة فى إصداره إلى توافر التحريات الجدية(١).

فجدية التحريات هى المعيار اللازم لمباشرة بعض إجراءات التحقيق(**) وذلك بشأن الجريمة التقليدية، وبالتالى قياساً يكون حرياً بمأمور الضبط القضائى أن يتوافر لدية مقدراً من العلم والمعرفة بتقنيات المعلوماتية، تصبغ تحرياته بشأن الجريمة المعلوماتية بالجدية المطلوبة، ونتلمس سبيل هذه المعرفة وأسس ذلك العلم، من أن معيار جدية التحريات يقوم على أساس توافر شرطين هما:

---

(*) إذ لمأمور الضبط القضائى أن يستعين فيما يجريه من تحريات وأبحاث أو ما يتخذه من وسائل التنقيب بمعاونين من رجال السلطة العامة والمرشدين السريين، ومن يتولون ابلاغه عما وقع بالفعل من جرائم. (المرجع السابق – ص ١١٨).
كما وأن القانون لا يجوب حتما أن يكون رجل الضبط القضائى قد أمضى وقتاً طويلاً فى التحريات، فله أن يأخذ بما يجريه رجال السلطة العامة والمرشدين السريين من تَنَقِّيب عن الجرائم، مادام أنه قد أقتنع شخصيا بصحة ما نقلوه إليه. (الطعن رقم ١٢٨٤ لسنة ٤٨ق – جلسة ١٩٧٨/١٢/٧ – س ٢٩ ص ٨٧٩ الموسوعة الذهبية للقواعد القانونية – ص ٣١ قاعدة ٦٦).

(١) د/ إبراهيم حامد طنطاوى – سلطات مأمور الضبط القضائى – المكتبة القانونية – القاهرة، ط٢، سنة ١٩٩٧، ص ٢٦٧.

(**) ذهبت محكمة استئناف القاهرة إلى القول بأن القانون لم يضع معياراً تقاس به جدية التحريات من عدمها، إذ أن ذلك من اطلاقات النيابة العامة، لها أن تطمئن إليها أو لا تطمئن دون أسباب. (جلسة ١١ أبريل سنة ١٩٩٠ – الطعن رقم ٣٠٣٠ لسنة ١٩٨٩ – غير منشور).

- تعلق التحريات بجريمة وقعت بالفعل.
- وتوافر الدلائل والامارات الكافية التى ترجح نسبة الجريمة المرتكبة إلى المشتبه فيه.

وبمعنى أوضح فإن جدية التحريات تعنى ضرورة أن تنأى – تبعد – عن مجرد الهواجس أو الأوهام أو الظنون والأحلام أو التخيلات التى قد تطفو فى ذهن مأمور الضبط القضائى الذى يسعى إلى القيام بها، وانما هى – وكما يجب أن تكون – خلاصة عملية ذهنية تمخضت عنها تحريات واستدلالات واستخبارات توحى جميعها بقدر من الامارات والقرائن والدلائل المستمدة من وقائع تنتجها أصلاً وواقعاً. وفى الجملة ترجح ضرورة قيام الدواعى والأسباب التى توجب تدخل مأمور الضبط القضائى، إعمالاً لما تفرضه النصوص التشرعية عليه من واجبات[1]. وليس أدل على ذلك من الأهتمام الذى توليه أجهزة الأمن بالعنصر البشرى فى عمليات مكافحة الجرائم المعلوماتية كإحدى أهم مراحل المواجهة، حيث يلزم أن يكون القائم على مكافحة هذه النوعية من الجرائم على دراية تامة بآليات التعامل بها وأنواعها المختلفة، وفوائدها وأخطارها والقوانين والاعراف المنظمة لها[2].

**البند الرابع: محل تفتيش نظم المعلوماتية:**

نظم المعلوماتية بما تشمله من وعاء – محتوى – هو الحاسب بمكوناته وشبكات أتصاله، تستلزم مجموعة من الأشخاص ذوى الخبرة والتخصص

---

(١) لواء د/ قدرى عبد الفتاح الشهاوى – مرجع سابق – ص ١٠٥.
(٢) لواء/ نجاح محمد فوزى – وعى المواطن العربى تجاه جرائم الاحتيال (بطاقات الدفع الإليكترونى نموذجا) – مرجع سابق – ص ١٤٧.
وتجدر الاشارة أن إدارة مكافحة جرائم التزييف والتزوير بوزارة الداخلية المصرية، تضم وحدة للبحوث الفنية متكاملة التجهيزات وتقوم بتقديم الدعم الفنى للضباط فى مجال الاجرام المعلوماتى والجرائم ذات التقنية الحديثة منذ عام ١٩٩٤م.

المهنى فى التقنية التكنولوجيا المعلوماتية وهم مشغلو الحاسب Computer Aper-ators ، وخبراء البرمجة Program mers سواء كانوا مخططى برامج تطبيقا Ap-plication Programmers، أم كانوا مخططى برامج نظم Systems Program-mers ، والمحللين Analysts ، ومهندسوا الصيانة والأتصالات، ومديرى النظم المعلوماتية[1]:

وعلى ما تقدم يمكن القول ان محل التفتيش نظم المعلوماتية هو:

- مكونات الحاسب الآلى المادية والمعنوية، وشبكات الاتصالات به، والتى قد توجد فى حوزة شخص، أو تكون موضوعة فى مكان له حرمة المسكن.

لذا فإنه من الحرى بنا أن نوضح المقصود بالشخص كمحل للتفتيش فى جريمة معلوماتية، وبيان المقصود بالمكان الذى له حرمة المسكن والكائنة به المكونات التى تمثل المحتوى للمعلوماتية.

**أولاً: المقصود بالشخص كمحل لتفتيش نظم المعلوماتية(*):**

قد يكون هذا الشخص من مشغلى أو مستخدمى الحاسب، أو مقدمى الخدمة أو من خبراء البرامج سواء كانت برامج نظام أم برامج تطبيقات، أو من المحللين، أو من مهندسى الصيانة والاتصالات، أو من مديرى النظم

(١) للمزيد بشأن البرمجة يراجع: مهندس/ على يوسف على - محجم مصطلحات الحاسب - مرجع سابق - ١٩٩٩ - حرف p - ص ٥٣٦ وما بعدها.

(*) يخرج من نطاق الدراسة تفتيش الأشخاص الذين يتمتعون بحصانات معينة، كأعضاء السلك الدبلوماسى، وأعضاء المجالس النيابة والقضائية، حتى يتم رفع الحصانة عنهم، فيتم تطبيق القواعد الاجرائية العامة بشأنهم. وللمزيد من المعرفة بشأن القواعد العامة لتفتيش الأشخاص يراجع:

أ/ أحمد عثمان حمزاوى - مرجع سابق - ص ٢٩٥ وما بعدها. شرح وتفسير المواد ٤٥ وما بعدها إجراءات جنائية التى تضمنها الفصل الرابع (فى دخول المنازل وتفتيشها وتفتيش الاشخاص) - من الباب الثانى (فى جمع الاستدلالات ورفع الدعوى).

المعلوماتية، وبصفة عامة.. أى أشخاص آخرين يكون بحوزتهم أجهزة أو معدات معلوماتية، أو تليفونات محمولة متصلة بجهز المودم أو مخرجات أو مستندات أو أكواد، وحديثاً ظهرت معدات معلوماتية يمكن من خلالها ممارسة النشاط المعلوماتى مثل[١]:

حاسوب حقيبة Lap Top.

حاسوب مفكرة Note book خفيف للغاية Ultralignt[*].

حاسوب محمول باليدHandheld, Palmtop.

وفى كل الأحوال يقصد بالشخص المعلوماتى كمحل قابل للتفتيش كل ما يتعلق بكاينه المادى وما يتصل به، ويشمل جسم الإنسان وملابسه وامتعته التى كانت فى حوزته متنقلا بها باعتبارها من توابع الشخص، فتستمد حرمتها من هذه الحيازة ولو لم تكن ملكه. ولا يشترط أن تكون هذه الامتعة فى يد المتهم وقت تفتيشه لإمكان تفتيشها، بل يصح تفتيشها ولو كان يضعها أمامه فى الطريق العام، طالما أن ظاهر الحال لا يوحى بتخليه عنها[**]، كما لا يشترط أن تتخذ هذه الأمتعة شكلاً معيناً فقد تكون فى شكل حقائق أو صناديق أو لفائف... أو غير ذلك من أشكال تفيض عن الحصر[٢].

ويثور تساؤل، هل يدخل فى مضمون هذه الأمتعة السيارة التى قد

(١) مهندس/ على يوسف على – المرجع السابق – ص ٥٢٣.

(*) يمكن وضعه فى حقيبة مع بقية محتوياتها، وقد يكون له بدلاً من الاقراص الصلبة والمرنة.

(**) إذا تخلى الشخص عما يحوزه من أمتعة طواعية واختياراً، وكانت هذه الامتعة تحوى مكونات وأدوات معلوماتية، فإن هذا التخلى يجيز البحث والتنقيب فى هذه المعدات والمكونات المتخلى عنها، بحيث إذا أسفر البحث والتنقيب عن وجود جريمة معلوماتية متلبس بها، وتوافرت الدلائل الكافية قبل المتهم المعلوماتى على أنه مرتكبها جازّ تفتيشه. (يراجع فى أصل ذلك، نقض ٢٧ فبراير سنة ١٩٦١ – مجموعة أحكام النقض – س ١٢ – رقم ٥١ – ص ٢٨٠، نقض ١٧/١٠/١٩٦٠ – أحكام النقض – س ١ – رقم ١٣ – ص ٦٨٣.

(٢) د. هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢٦.

يستخدمها الشخص فى فعل أو إخفاء الأجهزة المعلوماتية، وبالتالى تعتبر امتداداً لشخصه، فتخضع للقواعد المتعلقة بتفتيش الأشخاص؟

أختلف الفقه عموماً فى حكم تفتيش السيارة، وهل تخضع لقواعد تفتيش الأشخاص؟ أم لقواعد تفتيش المنازل وما فى حكمها؟ على ثلاثة أراء نعرضها فى النطاق الذى يفيد الدراسة ويثريها[1]:

**الرأي الأول:** ذهب إلى أن السيارة لا تنطبق عليها قواعد تفتيش الأشخاص، وإنما تخضع لقواعد تفتيش المنازل. فالسيارة تتمتع بحرمة المسكن سواء كانت فى داخل المنزل أم فى خارجه[2].

**الرأي الثاني:** ينظر إلى طبيعة المكان الموجودة به السيارة الخاصة، وهل هو مكان عام أم مكان خاص له حرمة المسكن[3].

فاذا كانت السيارة الخاصة تسير فى طريق عام، تدخل فى مفهوم الأمتعة التى تعتبر أمتداد لشخص صاحبها، وتخضع بالتالى لقواعد تفتيش الاشخاص.

واذا كانت تقف فى مكان خاص له حرمة المسكن – فناء أو حديقة بمنزل المتهم – تخضع لقواعد تفتيش المنازل.

**الرأي الثالث:** ويذهب اليه أغلب الفقه نحو إسباغ أحكام تفتيش الأشخاص على السيارة بصفة عامة. فالسيارة ليست مسكناً سواء كانت داخل أو خارج المنزل.

وفى ذلك أيضاً ذهب القضاء، حيث قضت محكمة النقض المصرية بأنه:

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢٧ .

(٢) أ/ على ذكى العرابى – المبادئ الأساسية للتحقيقات والاجراءات الجنائية – مطبعة التأليف والترجمة والنشر – القاهرة سنة ١٩٤٠ – ص ٢٠٤ – هامش رقم ٤ .
وللمزيد بشأن أحكام تفتيش السيارة يراجع: أ/ أحمد عثمان حمزاوى – مرجع سابق – ص ٣٠٧ وما بعدها.

(٣) د/ إبراهيم حامد مرسى طنطاوى – مرجع سابق – ص ٧٨٣ وما بعدها.

«إذا ما صدر أمر النيابة بتفتيش المتهم فإنه يشمل بالضرورة ما يكون متصلا به، والسيارة الخاصة كذلك»[1]، وقد سبقت محكمة النقض الفرنسية فى الأخذ بهذا الرأى(*).

وفى كل الحالات، فإن تفتيش الشخص المعلوماتى يعنى تحسس ملابسه، كما يعنى فحص تلك املابس بدقة واخراج ما يخفيه الشخص فيها، ويعنى أيضاً فحص الجسد فحصاً ظاهرياً لضبط ما يكون لاصقا به من متحصلات الجريمة المعلوماتية(**).

---

(١) نقض ١٤ فبراير سنة ١٩٨٤ مجموعة أحكام النقض - س ٣٥ - رقم - ٣ - ص ١٤٩.

(*) وذلك منذ قانون التحقيق الجنائى. حيث قضت بأن: «عملية التفتيش الذى قام بها مأمور الضبط القضائى فى سيارة يقودها المتهم وهو خارج مسكنه لا تعتبر من قبيل عمليات التفتيش الخاضعة لأحكام تفتيش المنازل المقررة فى المادة ٣٧ من قانون التحقيق الجنائى (المادة ٥٦ من قانون الإجراءات الجنائية الحالى). وإن ضبط أشياء مسروقة تم اكتشافها داخل هذه السيارة لا تنطبق عليها أحكام المواد ٣٧، ٣٨، ٣٩ من قانون التحقيق الجنائى (المادة ٥٦ وما بعدها من قانون إ - جـ الحالى).

- Cass crim. 11 Sept. 1933, D.P. 1937-1-40-note G.L.

بل قررت صراحة أن مفهوم المنازل لا يشمل السيارة سواء فى أحكامها القديمة أم الحديثة.

- Cass. Crim, 8 Nov. 1979. d. 1980. IR. 523. obs. PUECH. JCP 1980- – 11-1933-7 Note DAVID.

وهذا هو الرأى الراجح على أساس أن السيارة لم تصنع بحسب الأصل لأن تكون مسكناً.

- Cass. Crim. 11 Sept. 1933. D.P. 1937-1-40-note G.L.

وبالنسبة لوسائل النقل العام كالقطارات وعربات المترو والترام والأتوبيسات، فإنها تعتبر فى حكم المحال العامة، والتى يجوز لكل شخص أن يستخدمها دون تمييز، ويمكن لمأمور الضبط القضائى دخولها لمراقبة تنفيذ القوانين واللوائح. دون تفتيش للركاب والامتعة ما لم تتوافر حالة تلبس بجريمة، تخول لمأمور الضبط سلطة القبض والتفتيش. (د. هلالى عبد اللاه أحمد - المرجع السابق - ص ١٢٩)

(**) ذهبت بعض المحاكم فى فرنسا إلى ايراد تحفظ بالنسبة لعبارة تحسس الملابس - إذ فرقت بين الملامسات أو التحسسات البسيطة Les Palpations sommaires والتفتيش البدنى La Fouille à Corps، فاستبعدت ا لنوع الأول من الخضوع لأحكام تفتيش الأشخاص.

- Paris, 12 Janvier 1954, D. 1954-11-C.A. Aix- en- Provence, 28 Juin, 1978, G. P. 1979, No. 52-53. J.C. 17.

-/-

**ثانياً: المقصود بالمنازل وما في حكمها كمحل للتفتيش المعلوماتي:**

**- الوضع في فرنسا[١]:**

نصت الفقرة الأولى من المادة ٧٦ من دستور ٢٢ فريمير Frimaire للسنة الثامنة VIII للثورة[٢] على أن: «منزل كل مواطن يقطن الاقليم الفرنسى ملجأ حصين».

"La Maison de toute Personne Habitant Le territoire Français est un'Asile Inviolable"[٣]

**المقصود بمصطلح المنزل:**

ورد بالفقرة الثالثة من المادة ١٠٤ من المنشور الدورى الصادر فى ١٧ فبراير سنة ١٩٦١، تفسيراً للمادة ٥٦ من قانون الإجراءات الجنائية الفرنسى قولها:

«إن المادة ٥٦ قد استخدمت كلمة المسكن Domicile كى تشير إلى كل محال الإقامة Toutes Les Résidences للأشخاص المشتبه فيهم أو أولئك الذين يحوزون أشياء تتعلق بالجريمة. قانون التحقيق الجنائى سبق أن تضمن نفس المصطلح، وأن القضاء سبق أن اعتبر هذا المصطلح يمتد ليشمل كافة محال الإقامة وكافة محال المأوى Tous Les Logements التى يشغلها الأشخاص

---

= ولكن هذه التفرقه انتقدها الفقه لسببين:

**أولهما**- صعوبة التفرقة بين النوعين، إذا أن تحسس ملابس المتهم يمثل أولى مراحل التفتيش.

**ثانيهما**- إن هذا التحسس ينطوى على اعتداء على حق الإنسان فى السرية أو على حرمة السر التى يكفلها القانون للإنسان، والتى لا يمكن كشفها إلا فى ضوء الضوابط المحددة قانوناً.

- PARRA et Montruil: "Traité de Police Judiciaire", Préface de R. MARCELLIN, Auillet, Paris, 1970, p. 250.

(١) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٢٩ وما بعدها.

(2) Constitution de la République française du 22 Frimaire an VIII.

(3) droit cons Itutionnel. p. 314.

المشتبه فيهم. إن كل ذلك يدعو إلى الاعتقاد بأن النص الجديد يجب أيضاً أن يتم تفسيره هكذا[(١)].

وتطبيقاً لذلك يدخل فى مفهوم السكن.. الشقة L'Appartement، غرفة فى فندق للإقامة المؤقتة Chambre d'hotel occupeé Temporairement، الخيمة Tente، الكارفان Car avane وهى عبارة عن غرفة متنقلة داخل مقطورة السيارة، المكتب Bureau[(٢)].

كما يدخل فى حكم المسكن المكان المهيأ للسكنى Habitation Lieu Destiné، وإن لم يكن مسكوناً بالفعل كمنزل الاصطياف أو المشتى. وكذلك يدخل فى هذا المفهوم الملحقات Dépendances المخصصة لمنافع هذا المسكن كغرف الغسيل وحظائر الدواجن والمطابخ والجراچات وحديقة المنزل وأفنيته المغلقة طالما كانت تابعة للمنزل ومتصلة ويضمها مع المنزل سور واحد[(٣)].

وقد حكمت محكمة النقض الفرنسية فى أحد القضايا بأن: «فناء المبنى» Une cour d'immeuble لا يعتبر فى حكم المسكن Domicile إذا كان غير مغلق Lorqu' elle n 'est pas close[(٤)].

---

(1) Code de Pracéd ure pénale. Dolloz. 1995 - 1996, p. 115

وقد عرف قانون العقوبات الفرنسى – الملغى – المسكن فى م ٣٩٠ وهو بصدد تشديد العقوبة عى السرقة من المساكن. وأقتبس منها المشرع العقابى المصرى الفقرة الأولى من المادة ٣١٧ عقوبات التى تشدد العقوبة على السرقات التى تحصل «فى مكان مسكون أو معد للسكن أو فى ملحقاته». ثم جاء قانون العقوبات الفرنسى الجديد – المعمول به اعتباراً من أول مارس لسنة ١٩٩٤– ونص فى الفقرة السادسة من المادة ٣١١ – ٤ على المحل المسكون وعلى الأماكن الأخرى.

(2) Casse - Crime. 24 Juin 1987. Bull. Crime. no. 267, cass. crime. 31 Janv. 1914, S. 1916.I.59.

(٣) الأستاذ/ جندى عبد الملك – الموسوعة الجنائية – مطبعة الاعتماد – القاهرة – سنة ١٩٤٢ – جـ٤ – بند ٢١٧.

- GARCON: "Code Pinal Annote". art. 381. nos 75 - 84.

(4) Cass. crim. 26 Sept, 1990, Bull. Crime, No. 321.

- الوضع في مصر:

لم يتناول المشرع تفسير المقصود بالمنزل عند تناوله – فى الفصل الرابع من الباب الثانى من القانون ١٥٠ لسنة ١٩٥٠م بإصدار قانون الإجراءات الجنائية – التنظيم القانونى العقابى لدخول المنازل وتفتيشها. (المواد من ٤٥ إلى ٦٠ أ – ج).

واجتهد الفقه فى تحديد هذه المسألة، فذهب رأى إلى أن: «المقصود بمنزل المتهم كل مكان مسور يستخدم للسكن، وسواء كان استعماله للسكن بصفة دائمة أو بصفة مؤقتة». واستطرد أنه أكثر من هذا أن القانون يحمى المحل المعد للسكن فقط، وإن كان لا يستخدم للسكن لا بصفة دائمة ولا بصفة مؤقتة، كالشقة الخالية المعروضة للايجار[١]. وأن العبرة فى تحديد المسكن بالصلاحية للاقامة والنوم ولو كان غير معد فى الأصل لذلك، وأنه لا عبرة فى هذه الحماية بسند الحيازة، فيستوى ما إذا كان سندها هو الملكية أو الإجارة أو الإنتفاع أو الارتفاق أو التسامح، وأيضا لا عبرة بمدة الإقامة طالت أم قصرت، فالحجرة فى فندق والمستأجرة للإقامة يوماً واحداً تعتبر سكناً[٢]. ويلحق بالمسكن ملحقاته أو توابعه، وهى الامكنة المتصلة بالمحل المسكون والمخصصة لمنافعه، سواء أكانت فوق سطحه أو تحت أرضه أو بجواره(*).

فيما ذهب رأى فقى أخر إلى أن كلمة منزل تنصرف إلى المنزل المسكون، والمعد للسكن والشقة الخالية من ساكنيها لغيابهم[٣].

(١) أ/ أحمد عثمان حمزاوى – مرجع سابق – ص ٣٠١.
وقد أضاف، أن القضاء الفرنسى أعتبر السفن والقوارب مساكن، بل توسع فى ذلك إلى حد اعتبار البنوك والكنائس من المساكن، مادام يقيم فيها ولو شخص واحد كالحارس أو البواب.

(٢) نقض فرنسى ٣١ يناير سنة ١٩١٤ – داللوز سنة ١٨٩١ -١-٧٦، جارسون مادة ١٨٤ ن ٧-١٦، وجارو – جـ٤–ن ١٥٤٥، والعرابى – جـ١– ص ٢٥٤.

(*) وأن حماية الملحقات على الوجه المقرر للسكن مقيدة بأن يكون الانتفاع بها خاصاً، ولا يسمح للجمهور بارتياد هذه الملحقات.

(٣) د/ رءوف عبيد – مبادئ الإجراءات الجنائية (فى القانون المصرى) – دار الفكر العربى – القاهرة – ط ١٦ – سنة ١٩٨٥ – ص ٣٧١.

وقد أدلى القضاء بدلوه فى هذه المسألة، ففى قضاء حديث لمحكمة النقض نجدها تضفى حصانة المنزل المسكون على المتجر عند غيابه صاحبه نفسه، حتى ولو كان بابه مفتوحاً أثناء النهار، حيث قضت بأن[1]: «للمتجر حرمة مستمدة من اتصاله بشخص صاحبه أو بمسكنه....».

وتأسيساً على ذلك إذا وجدت مكونات نظم المعلوماتية سواء كانت مادية أو معنوية أو شبكات الاتصال الخاصة بها، فى فيلا أو منزل أو كوخ، أو فى أحدى الشقق، أو غرفة فى فندق لأحد النزلاء، أو فى خيمة ضاربة فى الصحراء، أو فى كارفان، أو فى شاليه. أو كانت مخبأة فى أحد الجراجات الخاصة المغلقة وما شابهها، فإن تفتيش هذه الأماكن يخضع لقواعد تفتيش المنازل[2]. أما اذا وجدت مكونات نظم المعلوماتية فى غير هذه الأماكن، فإن تفتيشها يخضع لقواعد تفتيش الأشخاص(*).

---

(١) نقض ٢٦ فبراير سنة ١٩٧٨ – أحكام النقض – س ٢٩ – رقم ٣٢ – ص ١٨٥.

(٢)د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ١٣٢.

(*) لا يدخل فى مفهوم السكن السيارة Le véhicule. Automobile

- Cass-Crim- 8 Nov. 1978, D- 1980. IR. 523. obs. PUECH, JCP. 1980, II-1932-7 note DAVIA.

ومقر الشركة Siége D'une Association

- Cass. Crim. 27 Sept, 1984 Bull - crime. no. 275.

وخزانة أمانات المحطة Cass. Crim. 12 Oct. 1993, Bull. Crime. no, 287, D. 1993, IR. 252.

وقضت محكمة الإستئناف بأنه لا يعتبر مسكناً قارباً طوله خمسة أمتار، ليس فيه أيه تجهيزات يجعله شبيهاً بأى يخت للنزهة.

- Cass. Crim. 20 Nov. 1984. Bull. Crime. no, 355,

أما إذا كان بالقارب أو الزورق محلاً مخصصاً للسكن، فإنه يعد من قبيل المسكن. (استئناف مصر فى ١٦ مارس سنة ١٨٩٧ مجلة القضاء – س ٤ – ص ١٩٩).

**البند الخامس: السلطة المختصة بتفتيش نظم المعلوماتية:**

**• أداة تخويل سلطة الضبط القضائي:**

تقتضى الشرعية الإجرائية أن يكون القانون هو المصدر للإجراءات الجنائية، ذلك بناء على كون هذه الإجراءات بحسب طبيعتها تمس الحرية الشخصية، الأمر الذى يتطلب من القانون وحده الاختصاص بتحديدها، لأن المشرع هو صاحب الكلمة فى تنظيم استعمال الحريات العامة(١).

**والإجراءات الجنائية تنقسم إلى نوعين:**

**الأول: إجراءات عامة لا تمس الحرية الشخصية:** وهى تتعلق بالدعوى الجنائية من حيث تحريكها وانقضاءها وارتباطها بالدعوى المدنية إلى غير ذلك.

**الثاني" إجراءات تتعلق بضبط الجريمة:** ويشمل ذلك حالة التلبس بارتكاب الجريمة وإجراءات القبض والتفتيش، وهذه إجراءات بحسب طبيعتها تمس الحرية الشخصية.

هذا بالإضافة إلى أن القانون قد خول لسلطة التحقيق الابتدائى، انتداب مأمور الضبط القضائى لمباشرة بعض إجراءات التحقيق، وهى جميعها تمس الحرية الشخصية.

ولما كان تحديد سلطة الضبط القضائى ينطوى حتماً ولزوماً، على منح أصحاب هذه الصفة الاختصاص بمباشرة إجراءات جنائية تمس الحرية الشخصية، وكانت قواعد الاختصاص هى من صميم قواعد الإجراءات الجنائية، فإن ذلك يقتضى أن يكون القانون وحده هو الأداة الصالحة لتخويل سلطة الضبط القضائى. فضابط الشرطة عندما يمارس اختصاصه فى أعمال الضبطية القضائية، فإنه يستند فى ذلك إلى النصوص التشريعية التى خولته هذا الاختصاص.

---

(١) د/ أحمد فتحى سرور – الوسيط فى قانون الإجراءات الجنائية – مرجع سابق – ط٤ – سنة ١٩٨١ – ص ٦٠٠.

**أولاً: صفة الضبطية القضائية ونطاق اختصاصها:**

تعبير (مأمور الضبط القضائى) ترجمة تقليدية لعبارة Officier de la po-lice judiciarc ويقصد بها كل من أوكل له القانون مسئولية ضبط الوقائع، التى يضع لها القانون جزاءً جنائياً، وجمع الأدلة عليها وعلى من ارتكبها من ضبطه شخصياً فى بعض الظروف(1).

وقد عهد قانون الإجراءات الجنائية بمهمة الضبط القضائى بمقتضى المادة ٢١ إجراءات جنائية إلى مأمورى الضبط القضائى، ولما كان أداء هذه المهمة يتطلب أحياناً المساس بالحريات الشخصية للمواطنين، كان منطقياً أن يتم تحديد من يحوز تلك الصفة بمقتضى القانون، فلا يجوز تخويل - منح - تلك الصفة لأحد إلا بقانون، أو بمقتضى قانون(2).

- **تحديد مأموري الضبط القضائي:**

تنطوى إجراءات الضبط القضائى فى جانب منها على مساس بحريات الأفراد، لذلك يعمد المشرع إلى تحديد الأشخاص الذين يضفى عليهم صفة الضبطية القضائية، حتى يتيقن من ممارسة هذه الإجراءات من جانب أشخاص موثوق فيهم.

***ويجمع المشرع عادة بين طريقتين في منحه لصفة الضبطية القضائية:***

أولاً: أن يحدد الأشخاص الذين تثبت لهم هذه الصفة، بحيث يكون هذا التحديد فى صلب القانون.

ثانياً: يخول الوزير المختص إضفاء هذه الصفة على بعض موظفيه بالنسبة

---

(1) د/ حسن علام - قانون الإجراءات الجنائية - الجزء الأول - المجلد الأول - مطابع روز اليوسف - القاهرة - سنة ١٩٨٢ - ص ٨٠.

(2) د/ محمد زكى أبو عامر - الإجراءات الجنائية - دار المطبوعات الجامعية - سنة ١٩٨٤ - ص ١١٧.

للجرائم المرتبطة بوظائفهم، وأيا ما كانت الطريقة التى تبعها المشرع فى تحديد من له صفة الضبط القضائى، فإن إجراءات الضبط القضائى لا يمكن مباشرتها إلا من جانب من تثبت له هذه الصفة، وإلا كانت هذه الإجراءات باطلة[1] .

**وفي هذا المعني قضت محكمة النقض في أحد أحكامها:**

«حيث أن مما ينعاه هذا الطاعن على الحكم المعطون فيها، أنه قضى بإدانته استناداً إلى تفتيش باطل، ولم يأخذ بما دفع به من البطلان الناشئ عن كون الضابط الذى أجراه هو ضابط مكتب مكافحة المخدرات بالإسكندرية، التابع لإدارة مكافحة المخدرات التابعة لإدارة الأمن العام بالقاهرة، وذلك بأن الإدارة العامة لمكافحة المخدرات لم تنشأ بالطريق القانونى الصحيح، ولا تتوافر لرجالها صفة مأمورى الضبطية القضائية، وبالتالى فليس لضابط المكتب المشار إليه الصفة التى تخوله حق أجراء التفتيش الذى قام به، لذلك يتعين نقض الحكم»[2] .

---

(١) د/ إبراهيم حامد طنطاوى – مرجع سابق – ص ١٤٢.

وتطبيقاً لذلك قضى بأنه: «ولما كان ضباط مكاتب الآداب لم يمنحوا هذه الصفة أى – مأمورى الضبط القضائى – إلا فى ٢٤ ديسمبر ١٩٥٢، فأنه متى كان ضابط مكتب الآداب قد قام بالتفتيش فى وأقعة الدعوى قبل أن يمنح صفة الضبطية القضائية فى ٢٤ من ديسمبر سنة ١٩٥٢ فان تفتيشه يكون باطلاً وكذلك الدليل المستمد منه» نقض ٢١ ديسمبر سنة ١٩٥٣ أحكام محكمة النقض – س ٥ – رقم ٥٨ – ص ١٧١.

وفى نفس المضمون راجع: أ/ أحمد حمزاوى – التعليق على قانون الإجراءات الجنائية – دار النشر للجامعات المصرية – سنة ١٩٥٣ – ص ١٩٦، د/ عبد الرءوف مهدى – شرح القواعد العامة للإجراءات الجنائية – القاهرة – مرجع سابق – ٢٠٠٢ – رقم ١٠٤ – ص١٩٣.

(٢) حكم محكمة النقض الصادر فى ١٩ يونيه سنة ١٩٥٢ فى القضية المقيدة بجدولها برقم ١٠١– سنة ٢٢ قضائية.

وبالنسبة لتحديد من منحهم القانون هذه الصفة، فقد تولت المادة ٢٣ من قانون الإجراءات الجنائية المصرى ذلك(*)، وحصرت هؤلاء فى طائفتين:

**الطائفة الأولى:** تضم مأمورو الضبط القضائى ذوو الاختصاص النوعى العام لجميع أنواع الجرائم، وقد ورد تعدادهم على سبيل الحصر فكان اختصاصهم بمباشرة مهمة الضبط القضائى (بقانون).

**الطائفة الثانية:** تضم مأمورو الضبط القضائى ذووا لاختصاص – النوعى – الخاص بجرائم معينة تتعلق بوظائفهم التى يباشرونها أصلا، وهؤلاء يكتسبون هذه الصفة بمقتضى (قرار يصدر من وزير العدل بالاتفاق مع الوزير المختص)، وذلك إعمالاً لنص المادة ٢٣ من قانون الإجراءات الجنائية.

**الطائفة الأولى: مأمورو الضبط القضائي ذوو الاختصاص النوعي العام لجميع أنواع الجرائم:**

**فتنقسم إلي قسمين:**

**القسم الأول:** ويتمتع بصفة الضبطية القضائية داخل نطاق جغرافى محدد، هو دائرة اختصاصهم المكانى ويضم:

١ – أعضاء النيابة العامة ومعاونوها(**).

٢ – ضباط الشرطة(١) وأمناؤها، والكونستبلات والمساعدين.

(*) تدخل المشرع بالتعديل فى هذه المادة أكثر من مرة بدأت بالقانون ٢٤٣ لسنة ١٩٥٣، ثم القانون رقم ٤ لسنة ١٩٥٤، ثم القانون رقم ٣٧ لسنة ١٩٥٧، ثم القانون رقم ٧ لسنة ١٩٦٣، وأخيراً القانون رقم ٢٦ لسنة ١٩٧١.

(**) لم يكن معاونوا النيابة العامة من مأمورى الضبط القضائى عند صدور قانون تحقيق الجنايات، حيث لم يرد النص عليهم فى المادة الرابعة من هذا القانون، وبتاريخ ٢٨ فبراير ١٩١٤ صدر أمر عال أضفى صفة الضبط القضائى عليهم، وأصبح معاونوا النيابة من مأمورى الضبط القضائى بموجب القانون رقم ٧ لسنة ١٩٦٣. (راجع فى ذلك: أ/ أحمد نشأت – شرح قانون تحقيق الجنايات – القاهرة – مطبعة نصر – ط ٢ – جـ١ – سنة ١٩٢٩، ص ١٣).

(١) نقض ٦ أكتوبر ١٩٥٩ – أحكام محكمة النقض – س ١٠ – ق ١٦٤ – ص ٧٦٧، وتضمن الحكم

=/=

٣- رؤساء نقط الشرطة.

٤- العمد ومشايخ الخفراء.

٥- نظار ووكلاء محطات السكك الحديدية الحكومية.

ويضاف إلى هؤلاء كل من: - مديرى أمن المحافظات - ومفتشى مصلحة التفتيش العام بوزارة الداخلية(١).

حيث أجاز لهم القانون أن يؤدوا الأعمال التى يقوم بها مأمورى الضبط القضائى، فى دوائر اختصاصهم (فهم إذن ليسوا من مأمورى الضبط القضائى، وان جاز لهم اتخاذ الأعمال المعهود إليهم بها)(٢).

**القسم الثاني:** ويشمل مأمورو الضبط القضائى ذوو الاختصاص النوعى العام لسائر أنواع الجرائم فى جميع أنحاء الدولة. وقد أشارت المادة ٢٣ إ - ج إلى هذا القسم بقولها:

**ويكون من مأموري الضبط القضائي في جميع أنحاء الجمهورية:**

١- مديرو وضباط إدارة المباحث العامة بوزارة الداخلية وفروعها بمديريات الأمن(٣).

---

= أن: ضباط البوليس فى المراكز والبنادر والأقسام بمقتضى المادة ٢٣ أ - ج من مأمورى الضبطية القضائية الذين لهم فى الدوائر التى يؤدون فيها وظائفهم اختصاص عام بشأن جميع الجرائم من جنايات وجنح ومخالفات، فإذا كانت المحكمة قد أثبتت بما أوردته من ظروف الدعوى، أن المتهم كان يسير بسيارته مخالفاً اللوائح، بسيره فى شوارع المدينة بسرعة أكثر مما تستلزمه حسن القيادة فى مثل هذه الظروف، الأمر الذى هو مما يستوجب على ضابط البوليس مراعاة تنفيذه، فإن استيقافه السيارة لاتخاذ ما يلزم بشأنها يكون صحيحاً.

(١) تعدل اسم «مصلحة التفتيش العام» إلى «الإدارة العامة للتفتيش» بموجب القرار الجمهورى رقم ١٨٤١ لسنة ١٩٧١. الجريدة الرسمية فى ١٩٧١/٧/٢٢ - العدد ٢٩، ثم عدل مرة أخرى إلى قطاع التفتيش والرقابة.

(٢) أضيفت هذه الفقرة بالقانون رقم ٧ لسنة ١٩٦٣.

(٣) تعدل اسم «الإدارة العامة للمباحث العامة» إلى مسمى «الإدارة العامة لمباحث أمن الدولة» بموجب القرار الجمهورى رقم ١٨٤١ الصادر لسنة ١٩٧١، ثم رفعت إلى مستوى قطاع ليصبح المسمى الخاص بها قطاع مباحث أمن الدولة.

٢- مديرو الإدارات والأقسام ورؤساء المكاتب والمفتشون والضباط وأمناء الشرطة والكونستبلات والمساعدون وباحثات الشرطة العاملون بمصلحة الأمن العام(*) وفي شعب البحث الجنائي بمديريات الأمن(**).

٣- ضباط مصلحة السجون(***).

٤- مديرو الإدارة العامة لشرطة السكة الحديد والنقل والمواصلات، وضباط هذه الإدارة[1].

٥- قائد وضباط أساس هجانة الشرطة.

٦- مفتشو وزارة السياحة[2].

تلك هي طائفة مأموري الضبط القضائي ذات الاختصاص النوعي العام لجميع أنواع الجرائم، منهم من يحوز هذه الصفة - مكانياً - في النطاق الاقليمي

---

(*) أنشئت مصلحة الأمن العام في ٢٩ يناير ١٩١٣، وكان يطلق عليها مسمى «إدارة عموم الأمن العام»، وفي ١١ فبراير ١٩٥٣ وافق مجلس الوزراء على تغيير اسمها وأصبحت تسمى «مصلحة الأمن العام»، راجع في هذا الموضوع:

- (إبراهيم الفحام - نشأن مصلحة الأمن العام - مجلة الأمن العام - يوليو ١٩٦٧ - ع ٣٨ - ص ٦٥ وما بعدها).

(**) ولاية ضباط شعب البحث الجنائي ولاية عامة مصدرها المادة ٢٣ إ - ج، انبساط تلك الولاية على جميع أنواع الجرائم حتى ما أفردت له منها مكاتب خاصة وإضفاء صفة الضبط القضائي على موظف بصدد جرائم معينة لا يسلب هذه الصفة من مأموري الضبط القضائي ذوي الاختصاص العام في شأن هذه الجرائم عينها. (نقض ١٩٧٢/٥/٢٨ - س ٢٣ - ق ١٨٢ - ص ٨٠٢، نقض ١٩٧٢/١٢/٣ - س ٢٣ - ق ٢٩٦ - ص ١٣١٧ مجموعة أحكام محكمة النقض).

(***) أنشئت مصلحة السجون بتاريخ ١٠ فبراير سنة ١٨٨٤، للمزيد في ذلك يراجع: «تطور نظام السجون وإصلاحها في مصر» - الكتاب الذهبي للمحاكم الأهلية (ب - ت) - جـ١ - القاهرة ص ٣٢١.

(١) ويدخل في اختصاصهم ضبط جميع الجرائم: نقض ١٣ مارس ١٩٧٧ - أحكام محكمة النقض - س ٢٨ في ١٦١، ص ٧٧٥.

(٢) معدلة بالقانون رقم ٢٦ لسنة ١٩٧١.

لدائرة اختصاصه فقط، ومنهم من يحوزها - مكانياً - فى النطاق الاقليمى للجمهورية كافة(1).

والتعداد السابق لأفراد هذه الطائفة وارد على سبيل الحصر، بما لا يجوز معه منح هذه الصفة لغيرهم دون تدخل تشريعى(*).

- **الطائفة الثانية: مأمورو الضبط القضائي ذوو الاختصاص المقيد بأنواع معينة من الجرائم:**

فقد أشارت إليم المادة ٢٣ إ - ج (ويجوز بقرار من وزير العدل بالاتفاق مع الوزير المختص تخويل بعض الموظفين صفة مأمورى الضبط القضائى بالنسبة إلى الجرائم التى تقع فى دوائر اختصاصهم وتكون متعلقة بأعمال وظائفهم)(2).

---

(1) نقض ٩ يوليو ١٩٥٣ مجموعة أحكام محكمة النقض - س ٤ - ص ١١٧٤. حيث ورد فى الحكم أنه:
(وإذا كان من قام بالتفتيش ضابطاً من ضباط مديرية أمن الدقهلية تابعاً مباشرة لمديرها وحكمدارها، فأنه بذلك تكون له صفة مأمورى الضبط القضائى بوجه عام بالنسبة لجميع الجرائم بدائرة المديرية، فإذا ندبته النيابة المختصة للتفتيش كان إجراؤه سليماً، ولا يؤثر فى ذلك إن يكون المدير أو الحكمدار قد كلف ذلك الضابط بالتحرى فى نوع معين من الجرائم أو خصصه فترة محددة للتحرى فى جرائم المخدرات ذاتها. سواء بالتعاون مع فرع إدارة المخدرات بالمديرية أو على وجه الاستقلال عنه، لأن إنشاء إدارة لمكافحة المخدرات تابعة لمدير الأمن العام لم ينزع اختصاص مدير أمن الدقهلية فى جرائم المخدرات التى تقع فى دائرة مديريته، وتكليف بعض مأمورى الضبط القضائى بضبطها مشتركين مع ضابط إدارة المخدرات أو مستقلين عنهم مما يدخل فى صميم تقديره هو).

(*) يجوز إذن من الناحية القانونية منح صفة مأمور الضبط القضائى لغير هؤلاء بقانون، وهناك عدة قوانين خاصة - من بينها (القانون رقم ١٨٢ لسنة ١٩٦٠ بشأن المخدرات) - تمنح صفة الضبطية القضائية على مستوى الجمهورية لأشخاص محددين بالنسبة لأنواع محددة من الجرائم كجرائم المخدرات فى القانون السابق ذكره.
انظر التطبيقات القضائية بشأن المادة ٤٩٥ من القانون ١٨٢ لسنة ١٩٦٠ فى شأن جرائم المخدرات أحكام محكمة النقض الآتية: نقض ٥ فبراير ١٩٦٨ أحكام محكمة النقض - س ١٩ - ق ٢٣ - ص ١٢٤، نقض ٤ أكتوبر ١٩٦٦ - س ١٧ - ق ١٦ - ص ٩١٨.

(2) مضافة بالقانون رقم ٣٧ لسنة ١٩٥٧، جريدة الوقائع المصرية فى ١٩٥٧/٢/٤ - ع ١١ مكرر.

وهؤلاء يتم منحهم صفة الضبطية القضائية بقرار من وزير العدل بعد الاتفاق مع الوزير المختص(*)، وقد قصر القانون تلك الصفة على دوائر اختصاصهم من جهة وعلى الجرائم المتعلقة بأعمال وظائفهم من جهة أخرى(١) .

وتجدر الإشارة إلى أن قيام أحد من غير مأموري الضبط القضائي بأي إجراء من الإجراءات المخولة في القانون لمأموري الضبط القضائي يكون باطلاً، ولو كان من قام بالإجراء واحداً من رجال الضبطية الإدارية، فصفة الضبطية القضائية لا تصبغ إلا بقانون – أو بمقتضى قانون(٢)، كما ينبغي أن يلاحظ أنه

---

(*) ينتقد الأستاذ الدكتور/ أحمد فتحي سرور منح هؤلاء صفة الضبطية القضائية «بقرار» لكن الواقع إن الضرورات العملية هي التي تفرض تلك الأداة، ثم إن هذا القرار وإن لم يكن قانوناً إلا أنه يصدر بناء على قانون ا لإجراءات الجنائية وفي حدود ما اشترط، وقد بررت المذكرة الإيضاحية ذلك بقولها: (نظراً لاضطراد وزيادة القوانين الجنائية الخاصة... رؤى تيسير إجراءات تعيين رجال الضبط القضائي)، راجع: د/ حسن صادق المرصفاوي – المرصفاوي في أصول الإجراءات الجنائية – الإسكندرية – منشأة المعارف – طبعة أخيرة – سنة ١٩٨٢ – ص ٢٥٢ .
وللمزيد يراجع أ/ أحمد عثمان الحمزاوي – المرجع السابق – ص ٢٠٠، حيث يضيف: وقد جرى العمل للأسف بعد صدور قانون الإجراءات الجنائية، على النص في القوانين المختلفة على أن من حق الوزير المختص بتنفيذها، أن يصدر قرارات وزارية تضفي صفة مأمور الضبط القضائي على من يشاء من موظفيه فيما يتعلق بالجرائم التي تقع مخالفة لأحكام ذلك القانون.
وقد حاربت هذه النزعة ما وسعني الجهد في مجلس الشيوخ، لأنها لا تتفق وما هدف إليه المشرع من النص على إن إضفاء تلك الصفة لا يكون إلا بقانون، يعرض على المجلس ليبدي رأيه فيمن يُمنح سلطة مأمور الضبط القضائي، التي تمس فيما تمس حرية الأفراد الشخصية ومساكنهم.

(١) وقد قضت محكمة النقض بأن: (مأمور الضبط القضائي ذوو الاختصاص الخاص مقصور اختصاصهم على جرائم معينة، يحددها لهم طبيعة وظائفهم، والحكمة التي من أجلها أصبغ القانون عليهم وعلى الهيئات التي ينتمون إليها كياناً خاصاً يميزهم) نقض ١٣ يونيه ١٩٧٧ – أحكام محكمة النقض س ٢٨ – ق ١٦١ – ص ٧٧٥.

(٢) أضاف المرسوم بقانون رقم ٣٥٨ لسنة ١٩٥٢ للمادة ٢٣ الفقرة الآتية: «مدير إدارة بوليس الآداب العامة، والضباط والصولات والكونستبلات الحائزون على دبلوم كلية البوليس في الإدارة العامة وفروعها في المحافظات والمديريات»، وذلك بعد فقرة قائد وضباط أساس هجانة الشرطة، راجع في ذلك: أ/ أحمد الحمزاوي – المرجع السابق – ص ١٨٦ .

وإن كان العمل يجرى على انفراد مأمورى الضبط القضائى ذوى الاختصاص الخاص بالضبطية القضائية بالنسبة للجرائم المتعلقة بوظائفهم، فإن ذلك لا يعنى تخصيصهم وحدهم بمباشرة الإجراءات الخاصة بتلك الجرائم، بل أن لكل من أفراد الضبط القضائى ذوى الاختصاص العام مباشرتها فى دائرة اختصاصه(1).

وبعد أن استعرضنا طائفتى مأمورى الضبطية القضائية، يتضح لنا جلياً أهمية تدخل المشرع الإجرائى، من أجل منح ضباط الإدارة العامة للمعلومات والوثيق صفة الضبطية القضائية والنص عليهم ضمن طائفة مأمورى الضبط القضائى المنصوص عليهم فى المادة ٢٣ إجراءات جنائية، وذلك صراحة دون النظر إلى الفقرة الثانية من ذات المادة، والتى تجيز منح بعض الموظفين صفة الضبطية القضائية بقرار من وزير العدل بالاتفاق مع الوزير المختص. وقد عرضنا لإختلاف الفقه فى هذا الشأن بين مويد ومعارض.

ولاشك أن أهمية المرحلة المعلوماتية القادمة، سوف يتعاظم فيها الخروج عن القانون وانتهاك الشرعية، مما يتحتم معه تدخل المشرع بكل حزم وصرامة قانونية، لإعادة تنظيم النصوص الإجرائية والمواد العقابية لمكافحة هذا المد الإجرامى للنظم المعلوماتية، واعتبار أن هذه الطائفة (من ضباط الإدارة العامة للمعلومات والتوثيق) موكول إليها الكثير والكثير من عبء هذه المواجهة.

**ثانياً: اجراء تفتيش نظم المعلوماتية:**

الصورة الأكثر شيوعاً أن يتم إجراء تفتيش نظم المعلوماتية بمعرفة مأمورى الضبط القضائى(*)، وذلك فى نطاق ضبط الجريمة المعلوماتية، ويتحقق ذلك فى حالات أربع هى:

---

(1) د/ محمد زكى أبو عامر – مرجع سابق – ص ١٢٣.

(*) جعل المشرع الإجرائى المصرى الاختصاص بالتفتيش كإجراء تحقيق – فى الجرائم التقليدية – للنيابة العامة بصفة أصيلة ولقاضى التحقيق فى حالات خاصة. ويتميز هذا الأخير عن النيابة العامة فى سلطته فى تفتيش المتهم وغير المتهم سواء فى شخصه (م ٩٤ أ – ج) أو منزله –/–

- التفتيش بناء علي اذن قضائي بإجرائه.
- التفتيش بناء على القبض على الأشخاص.
- التفتيش بناء على التلبس بالجريمة.
- التفتيش بناء على موافقة المتهم.

وفيما يلى سوف نعرض لهذه الحالات تباعاً، بالشكل الذى يفيد الدراسة:

**أ - تفتيش نظم المعلوماتية بناء علي أذن قضائي بإجرائه:**

من المستقر عليه أن سلطة التحقيق الأصيلة غير مطالبة بإجراء التفتيش بنفسها فى كل الحالات، بل لها أن تندب أحد مأمورى الضبط القضائى لإجرائه. وبناء على ذلك يمكن تعريف الأذن أو الأمر بالتفتيش بأنه:

---

-- (المادة ٩٣ أ - ج)، أما النيابة العامة فلا تملك ذلك بمفردها، بل يجب عليها لاتخاذ هذا الاجراء الحصول مقدماً على أمر مسبب بذلك من القاضى الجزئى بعد أطلاعه على الأوراق. ولا يكفى توافر صفة قاضى التحقيق أو عضو النيابة العامة لكى يقوم بهذا الاجراء فى جميع الحالات، بل لابد أن يكون مختصاً أصلاً بالتحقيق فى الجريمة، وبالاضافة إلى الاختصاص المكانى يجب توافر الاختصاص النوعى.

- وفى فرنسا، أناط القانون الفرنسى الاختصاص الأصيل بقاضي التحقيق.

- pradel (J.): "L'Instruction Préparatoire" Dolloz, 1990.

أما النيابة العامة فلا تختص بالتفتيش إلا فى حالات معينة كالتلبس.

- Ixème Congrés International de Droit Pènal, La Haye 1964, Rapports Publiés in R.I.D. p. 1965, no. 3et.

وعن التطورات التاريخية لدور النيابة العامة فى فرنسا يراجع:

- RASSAT (Michéle - Laure): "Le Ministére Public entre son Passé et son Avenir" Libr. Général de Droit et de Jurispru dence". Paris, 1967

ومتى اختص قاضى التحقيق بالدعوى، أصبح من حقه اجراء التفتيش على النحو الذى يراه مفيداً، فى كشف الحقيقة لدى المتهم أو لدى غيره دون قيد على سلطاته، إلا ما تعلق بحقوق الدفاع.

- وفى انجلترا فإن معظم الإجراءات الجنائية منوطة بالشرطة ما عدا بعض الجرائم التى تناط بالمدعى العام Director of Public Prosecution أو النائب العام At torney General.

«عبارة عن تفويض يصدر من سلطة التحقيق المختصة إلى أحد مأموري الضبط القضائي، مخولاً إياه إجراء التفتيش الذي تختص به أصلا تلك السلطة»[1].

ولذا ينبغي أن تراعى في اصداره وتحريره جميع القيود الخاصة بالندب أو الإنابة القضائية La Commission rogatoire [2].

والسائد فقهاً، وقضاء أن الأذن الصادر بالتفتيش يعد عملاً من أعمال التحقيق. ويبنى على ذلك أنه يرتب أثره في قطع مدة التقادم في الدعوى الجنائية[3].

ويجد الندب في التفتيش سنده القانوني في المادتين ٧٠، ٢٠٠ إجراءات جنائية مصري. ويقابلهما المواد ١٥١ - ١٥٥ من قانون الإجراءات الفرنسي[4].

---

(١) د/ هلالي عبد اللاه أحمد - مرجع سابق - ص ١٣٨.

(٢) لمزيد من المعرفة عن الإنابة أو الندب يراجع:

- PINGUET (J.P.): "Les Commissions Rogatoires du Juge d'instruction en Pénal Interne et en Droit Pénal International" Thése Nancy, 1989.

(٣) وقد ذهب البعض إلى أن الندب للتحقيق عملاً إدارياً يتعلق بنطاق ولاية القضاء.

- MARQUISET: "L'Acte d'instruction" R.D.P. 1957, p. 41.

في حين ذهب جانب آخر إلى أن الندب يعد عملاً مختلطاً فهو إداري ومن أعمال التحقيق.

- BOULOC (B>): "L'acte d'instruction" these Paris, 1965, p. 76 et. s.

يراجع في عرض وتفنيد هذا الأراء: د/ سامي حسني الحسيني - النظرية العامة للتفتيش في القانون المصري والمقارن - رسالة دكتوراه - كلية الحقوق - جامعة عين شمس - سنة ١٩٧٠ - دار النهضة العربية، سنة ١٩٧٢ - ص ١٠٧ وما بعدها.

(٤) عن الأحكام المختلفة للندب في فرنسا تراجع التطبيقات القضائية التالية:

- Casse. Crime. 9 Leve. 1993, Bull. Crime. no. 66.
- Casse. Crime. 14 Janv. 1992, Bull. Crime. no. 13.
- Casse. Crime. 13 Sept. 1986, Bull. Crime. no. 254.
- Casse. Crime. 9 fév. 1982, D. 1982, 544 note PRADEL, Bull. Crim. no.47.
- Casse. Crime. 9 Oct. 1980, d. 1981, 332. note PRADEL, JCP 1981, II. 18578 note Di MARINO, 13 Bull. Crime. no. 255.

حيث نصت المادة ٢٠٠ على أنه: «لكل من أعضاء النيابة العامة فى حالة إجراء التحقيق بنفسه، أن يكلف أى مأمور من مأمورى الضبط القضائى ببعض الأعمال التى من اختصاصه». كما أعطت المادة ٧٠ إجراءات معدلة بالمرسوم رقم ٣٥٣ لسنة ١٩٥٢ نفس الحق لقاضى التحقيق.

أما بالنسبة للانابة القضائية فى جرائم المعلوماتية على وجه الخصوص: -

- فنجد في المملكة المتحدة (على سبيل المثال): أن قانون اساءة استخدام الحاسب Computer Misuse Act - سابق الاشارة إليه - يشترط ضرورة الحصول على اذن قضائى للتفتيش بالنسبة للجرائم المدرجة فى القسم الأول، والخاصة بالدخول غير المصرح به على نظام الحاسب. ولابد أن ينبنى هذا الاذن على أسباب منطقية، للاعتقاد بأن الجريمة قد وقعت أو يشتبه فى وقوعها فى أماكن خاصة، وأن هناك أدلة متعلقة بهذه الجريمة يمكن الحصول عليها فى هذه الأماكن(١).

- وفي كندا، فإن حصول السلطات العامة على اذن قضائى للتفتيش والضبط يستند لنص المادة ٤٨٧ من القانون الجنائى الكندى. فهذا النص أعطى سلطة اصدار اذن لتفتيش وضبط أى شئ بما فى ذلك بيانات الحاسب، طالما تدوفر أسس معقولة بأن الجرم ارتكب أو يشتبه فى ارتكابه، أو أنه قد قصد فى أن يستخدم فى ارتكاب الجرم، أو أنه سوف يتيح دليلاً على وقوعه(٢).

كذلك هناك قوانين أكثرَ تخصصاً فى كندا تقدم قواعد تفصيلية تطبق على بيانات الحاسب فى حالات معينة. ومن ذلك على سبيل المثال المادة ١/١٦ من قانون المنافسة The Competition التى تقرر أن الشخص الذى حصل على أمر قضائى بالتفتيش وفقاً للقانون، له أن يستخدم أو يعمل على استخدام أى نظام

---

(1) WASIK (Martin): art. Cité, p. 641.
- FERBRACHE (David): op. cit., p. 233.
(2) PIRAGOFF (Donald K.): art. Cité, 241.

للحاسب الآلي، لتفتيش أي بيانات يحتويها أو متاحة لهذا النظام، كما يمكنه أن يستخرج أو يعمل على استخراج بيانات، في شكل مطبوع أو أي مخرجات أخرى. كذلك بمقدوره ضبط هذه المطبوعات أو المخرجات الأخرى، من أجل فحصها أو نسخ صورة منها[1].

- أما في مصر: فلا يوجد أي نصوص في الإجراءات الجنائية تتعلق بالانابة أو الندب لتفتيش النظم المعلوماتية - على اختلاف مكوناتها - وبالتالي فإنه لا تبقى أمام الاجتهادات الفقهية، سوى تطبيق النصوص التقليدية والمحصورة في المادتين ٧٠، ٢٠٠، وهذا ما دفع رأي فقهي إلى أضافة عبارة: «بما في ذلك الندب لتفتيش مكونات الحاسب الآلي إلى كلا من المادتين»[2]. وذلك على اعتبار أن الحاسب الآلي بمكناته يمثل محتوى المعلوماتية.

**ب- تفتيش نظم المعلوماتية بناء على القبض على الأشخاص:**

من الآثار المترتبة على القبض الصحيح - بصفة عامة - تفتيش شخص المتهم، حيث نصت المادة ٤٦ إجراءات جنائية على أنه[3]:

«في الأحوال التي يجوز فيها القبض قانوناً على المتهم يجوز لمأمور الضبط القضائي أن يفتشه. وإذا كان المتهم أنثى، وجب أن يكون التفتيش بمعرفة أنثى يندبها لذلك مأمور الضبط القضائي»[*].

---

(1) Ibid.

(٢) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١٤١.

(٣) نقض ١٣ نوفمبر سنة ١٩٨٦ - مجموعة أحكام النقض - سنة ٥٦ ق - رقم ١٦٩، ص ٨٧٨، نقض ٢٩ يناير سنة ١٩٨٦ - مجموعة أحكام النقض - س ٥٥ ق - رقم ٣٤ - ص ١٦٣.

(*) مناط تفتيش الأنثى أن يكون في المواضع الجسمانية التي تعد من العورات، والتي لا يجوز للقائم بتنفيذ الأذن الاطلاع عليها لما في ذلك من خدش لحياء الأنثى (نقض ١٥ أكتوبر سنة ١٩٨٦ - مجموعة أحكام النقض - س ٥٦ - رقم ١٤٦ - ص ٧٦، نقض ١٩٨٤/١/٣١ - أحكام النقض - س ٣٥ - رقم ١٩ - ص ٩٥.

أما إذا كان تفتيش المرأة بمعرفة مأمور الضبط القضائي لا ينطوي على مساس جزء منها يعد عورة، فإن هذا التفتيش يعد صحيحاً. (نقض ١٤ يناير سنة ١٩٨٦ - أحكام النقض - س ٥٥ - -/-

وعلة هذا النص أنه مادام يجوز التعرض لحرية الشخص بالقبض عليه، فإنه يجوز تفتيشه، فتفتيش الشخص أقل خطورة من القبض عليه. أو أن القبض على المتهم يتضمن اعتداء على حريته الشخصية يزيد منها التفتيش، فإذا أهدرت الحرية الشخصية بالقبض، فإن ذلك يستتبع التسليم بحق مأمور الضبط القضائى فى تفتيشه(١).

والسائد فى تفتيش المقبوض عليه طبقاً لنص المادة ٤٦ أ - ج. سالفة الذكر أنه يشمل التفتيش بالمعنى الفنى الدقيق، وذلك للبحث عن أدلة الجريمة التى فى حيازة المتهم وضبطها، والتفتيش الوقائى لتجريد هذا المتهم مما يحتمل أن يكون معه من سلاح خشية أن يستعمله فى المقاومة أو فى الاعتداء به على نفسه(٢). أو غيره أو على أى من أفراد الضبط.

ولا يختلف الأمر فى القانون الفرنسى أو فى القانون الأنجلو أمريكى. فمن المستقر عليه فى القانون الفرنسى جواز تفتيش المقبوض عليه، لتجريده مما قد يحمله من أسلحة، أو للبحث عن أدلة الجريمة التى تفيد فى كشف الجريمة(٣). كما يجيز القانون العام الانجليزى لرجل البوليس تفتيش المتهم المقبوض عليه

---

= رقم ١٤ - ص ٦٤، نقض ٢١ مايو سنة ١٩٧٢ - أحكام النقض - س ٢٣ - رقم ١٦٩ - ص ٧٥٩.

ويلاحظ أن الكشف عن المضبوطات فى مكان حساس من جسم المتهمة بمعرفة الطبيب لا يؤثر على سلامة الإجراءات، حيث ذهب قضاء النقض المصرى إلى أن قيام الطبيب بهذا الإجراء إنما كان بوصفه خبيراً، وأن ما أجراه لا يعد وأن يكون تعرضا بالقدر الذى تستلزمه عملية التدخل الطبى اللازمة لإخراج المخدر من موضع إخفائه فى جسم الطاعنة. (نقض ٤ يناير سنة ١٩٧٦ - مجموعة أحكام النقض - س ٢٨ ق - ص ٩).

(١) أ/ أحمد عثمان حمزاوى - مرجع سابق - ص ٢٨٣.

(٢) نقض ١٣ نوفمبر سنة ١٩٨٦ مجموعة أحكام النقض س ٥٦ - رقم ١٦٩ - ص ٨٧٨، نقض ٢٩ يناير سنة ١٩٨٦، مجموعة أحكام النقض - س ٥٥ ق - رقم ٣٤، ص ١٦٣.

(3) Bouloc: Thèse cité. p. 201.

بهدف ضبط ما قد يكون فى حوزته من أدوات وأوراق تتعلق بالجريمة، وأيضاً لتجريده مما قد يكون معه من سلاح(١). كذلك من المقرر فى القانون الأمريكى أن إجراء التفتيش يكون لتجريد المتهم من أدوات الاعتداء كما يكون بهدف ضبط أدلة الجريمة(٢).

وبالنسبة لعملية التفتيش بالمعنى الفنى الدقيق فى مفهوم المادة ٤٦ من قانوننا الإجرائى، فإنها تعنى الكيان المادى للشخص محل التفتيش وما يتصل به. ويشمل هذا المفهوم جسم الإنسان وملابسه، وأمتعته التى فى حوزته متنقلاً بها باعتبارها من توابع الشخص(٣).

ومن الأمثلة النموذجية للقوانين التى نصت على تفتيش نظم المعلوماتية بناء على القبض على الأشخاص قانون سوء استخدام الحاسب Computer Mis-use Act فى انجلترا ذلك أن الجرائم المدرجة فى القسمين الثانى والثالث من قانون سوء استخدام الحاسب يعاقب عليها عند الإدانه بعقوبة السجن لمدة خمس سنوات كحد أقصى. وذلك يعنى أن هذه النوعية من الجرائم تستدعى القبض على المتهم طبقاً لقانون الشرطة والإثبات الجنائى لسنة ١٩٨٤. وبالتالى لرجل الشرطة القبض على المتهم دون حاجة لصدور إذن بالقبض. كما أن له تفتيش

---

(1) ARGYLE. HAVERS and BENADY: "Phips of evidence" 10th., London,. 1963. p. 13.
- TURNER (J.W. Cecil): "Kenny S. Outines of criminal low" 19the. ed. cambridge 1966. p. 525.
- ANDREWS (J.A.): "Involuntory confession and illegaly obtained evidence in criminal cases"> The criminal law review 1963. p. 77.
- WILLAMS (Glanville): "The proof of guilt - Astudy of The English crminal Trial" Third editian, London, 1963, p. 195.

(2) CAREY: "les Critères minimum de La justice criminelle aux Etats unis" R.I.D. p. 1966, p, 77.

(٣) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ١٥٥.

محل إقامة المتهم بحثاً عن أدلة ذات قيمة تتعلق بالجريمة المعلوماتية التى تم القبض عليه بسببها[1].

ونظراً لعدم وجود قانون خاص بالجوانب الإجرائية المعلوماتية فى مصر، فإنه إزاء هذا الفراغ التشريعى يمكن الاجتهاد فى حدود النصوص الإجرائية التقليدية. وعلى ذلك يمكن القول إن نص المادة ٤٦ من قانوننا الإجرائى يتسع ليستوعب تفتيش نظم المعلوماتية بناء على إجراء القبض على الأشخاص.

وفى هذا الخصوص نشير إلى أن الشخص بوصفه محلاً لتفتيش نظم المعلوماتية قد يكون من مشغلى أو مستخدمى الحاسب، أو من خبراء البرامج سواء كانت برامج نظام أو برامج تطبيقات، أو من المحللين، أو من مهندسى الصيانة والإتصالات، أو من مديرى النظم المعلوماتية، أو أى من الأشخاص الذين يكون بحوزتهم أجهزة أو معدات معلوماتية، أو مخرجات أو مستندات أو أكواد أو غير ذلك مما يتعلق بالجريمة المعلوماتية محل البحث[2].

**جـ- تفتيش نظم المعلوماتية بناء على حالة التلبس بالجريمة:**

هناك بعض القوانين لا تسمح لمأمور الضبط القضائى بتفتيش منزل المتهم بناء على حالة التلبس بارتكاب الجريمة، مثل قانون الإجراءات المصرى بعد الحكم بعدم دستورية م ٤٧ منه، فى حين توجد قوانين أخرى تجيز لأعضاء الضبط القضائى تفتيش منزل المتهم فى حالة التلبس بالجريمة، كما هو الحال فى فرنسا. إذ تنص المادة ٥٦ فى فقرتها الأولى على أنه: إذا كانت الجناية من النوع الذى يمكن إثباته بواسطة ضبط أوراق ومستندات وغيرها من الأشياء الموجودة فى حوزة أشخاص تظن مشاركتهم فى الجناية، أو تكون بيدهم مستندات أو أشياء تتعلق بالأفعال الإجرامية المرتكبة، فإن ضابط الشرطة

(1) FERBRACHE (David): op. cit., p. 233.

(٢) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٥٦.

القضائية ينتقل عاجلاً إلى منزل أولئك الأشخاص لإجراء التفتيش وتحرير محضر بشأنه»[1]. وقد استعملت المادة ٥٦ كلمة أى مسكن للدلالة على محال إقامة المتهمين أو الحائزين لمستندات أو أشياء تتعلق بالجريمة، وكان قانون التحقيق الجنائي يستعمل نفس التعبير، وجرى القضاء الفرنسي على تفسيره تفسيراً واسعاً بحيث يشمل كل محل يشغله المتهم، وهو ما يجب الأخذ به في تفسير الفقرة الأولى من المادة ٥٦[2].

وفي إيطاليا، تنص المادة ٢٢٤ من قانون الإجراءات الجنائية على أن: «لمأموري الضبط القضائي - في حالة التلبس - تفتيش الأشخاص وأي مكان يكون لديهم مبرر للاعتقاد بأن المتهم قد لجأ إليه، أو أن به أشياء ينبغي ضبطها أو آثاراً يخشى عليها من العبث». غير أنه يجب على مأمور الضبط أن يبين في محضره السبب الذي حدا به إلى اتخاذ هذا الإجراء، وأن يرسل المحضر إلى سلطة التحقيق المختصة في خلال ٤٨ ساعة. وتصدق سلطة التحقيق على المحضر متى تحققت من صحة الإجراء[3].

وفي القانون الأنجلو أمريكي: يجوز تفتيش منزل المتهم في حالة التلبس. فقد قضي بأن لرجل البوليس أن يدخل في مسكن استطاع أن يرى من الخارج

(١) ومن التطبيقات القضائية لهذه الفقرة يراجع:

- G=Casse. Crime. 30 Mai 1980, d. 1981, 533 note JEANDIDIER, Gaz pal 1981.1.221, note SUZANNE.
- Trib corr, Vannes, 18 Fev. 1982, D. 1983, 130, note CHAMBON.
- Casse. Crime. 11 Juin 1985, Bull, Crime. No. 227.
- Casse. Crime. 27 Sept. 1984, Bull. Crime. No. 275.
- Casse. Crime. 27 Janv. 1987, Bull Crime. No. 41. d. 1987, Somm. 408, obs. PRADEL, d. 1988, 179, note, DAROLLE.

(2) Code de Procèdure pénale, Dallaz 1995, 1996, p. 110.

وراجع أيضاً: د/ محمود محمود مصطفى، جـ٢، التفتيش والضبط - مطبعة جامعة القاهرة - جـ٢ - سنة ١٩٧٨ - ص ٥٠.

(٣) د/ هلالي عبد اللاه أحمد - المرجع السابق - ص ١٥٩.

جريمة ترتكب فيه، وأن له الحق عندئذ فى ضبط أدلة الجريمة فى ذلك المسكن، إذ من غير المعقول أن يغلق عينيه عن الجريمة التى شاهد ارتكابها(١).

وبالنسبة لتفتيش شخص المتهم، فإن يجوز فى حالة التلبس القيام بهذا الإجراء. إذ إن حالة التلبس تجيز القبض وفقاً للمادة ٣٤ من قانون الإجراءات الجنائية المصرى، والقبض يجيز التفتيش وفقاً للمادة ٤٦ من نفس القانون. ولا يختلف الأمر فى القانون الفرنسى أو فى القانون الأنجلو أمريكى إذ يجيز التلبس القبض على المتهم وتفتيشه(٢).

أما فيما يتعلق بموقف قانوننا الإجرائى من تفتيش نظم المعلوماتية بناء على التلبس بالجريمة، فإنه لا يختلف كثيراً عما سبق عرضه بصدد تفتيش نظم المعلوماتية بناء على القبض على الأشخاص. إذ إنه فى مواجهة هذا الفراغ التشريعى فإنه يمكن الاجتهاد فى حدود النصوص الإجرائية التقليدية. وعلى ذلك يمكن القول بأن نص المادة ٣٤ من نظامنا الإجرائى يتسع ليستوعب تفتيش نظم المعلوماتية بناء على التلبس بالجريمة. وفى هذا الخصوص ذهب رأى إلى إن نص المادة ٣٤ من قانوننا الإجرائى يعطى لمأمور الضبط القضائى فى أحوال التلبس بالجنايات والجنح المعلوماتية التى يعاقب عليها بالحبس مدة لا تزيد على ثلاثة أشهر أن يأمر بالقبض على المتهم المعلوماتى الذى توجد دلائل كافية على اتهامه(٣).

والقبض يجيز التفتيش على النحو الذى بيناه فى الفقرة سالفة الذكر.

---

(1) Griffin V. State, 200 Md. 529, 92 2d.
- 743, Cert Den. 345 U.S. 907, 97L ed. 1343 SCT.
- State V. Br Yant, 150 N. W. 2d. 621, 625, 1967.

مشار إليه فى د/ سامى حسنى الحسينى – المرجع السابق – ص ١٦٣.

(2) BOULOC: Thèse Cité No. 299, p. 201.
- ARGYLE, HAVERES and BENADAY: "Phipson on evidence" 10 the, ed. London, 1960, p. 13.

(٣) رأى د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ١٦٠.

د - تفتيش نظم المعلوماتية بناء علي موافقة المتهم:

خارج نطاق التلبس بالجرائم التقليدية توجد حالات معينة يمكن فيها إجراء التفتيش، طالما تمت موافقة ذى الشأن على تفتيش شخصه أو منزله. وذلك بتنازله عن الحماية التى كفلها له القانون. فقد نصت الفقرة الأولى من المادة ٧٦ من قانون الإجراءات الجنائية الفرنسي - على خلاف قانوننا الإجرائى المصرى - بأن تفتيش المساكن وضبط الأشياء التى يمكن أن تكون متعلقة بالجريمة، لا يمكن أن يتم دون موافقة صريحة للشخص الذى يزمع إجراء التفتيش عنده(*).

- القواعد العامة بشأن الموافقة علي التفتيش[١]:

تقرر المادة ١٢٧ من المرسوم الصادر فى ٢٠ مايو سنة ١٩٠٣ أن تفتيش المسكن وضبط الأشياء المتعلقة بالجريمة، لا يجب أن يتم بدون موافقة صريحة تعطى بحرية وعن معرفة بالسبب، وتطبيقاً لذلك تقرر محكمة النقض الفرنسية أن موافقة الشخص ذى الشأن لا تكون صالحة ومنتجة لأثارها، إلا عندما تعطى عن بينة تامة بالسبب. وأن يكون الشخص عالماً بأن مرحلة التحقيق لم تبدأ بعد[٢].

(*) ومن تطبيقات محكمة النقض الفرنسية قولها إنه: لا يمكن بدون موافقة صريحة من الشخص الذى يجرى تفتيش مسكنه، أن يقوم مأمور الضبط القضائى بإجراء تفتيش قانونى،أو أن يقوم بالضبط إلا فى حالة التلبس بجناية أو جنحة، وفى غير ذلك تعتبر عمليات التفتيش والضبط باطلة، وأيضاً بطلان أى دليل ينجم عنها:

- Cass. Crim. 24 Juin 1987, Bull. Crime, No. 267.
- Cass. Crim. 30 Mai 1980, D. 1981, 533, note JEANDIER.

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١٦٠.

(2) Casse. Crime. 26 Juin 1958, Bull. Crime. No. 506, R.S.C. 1959, 145.
- Casse. Crime. 9 Juill. 1952, D. 1954, 110.
- Casse. Crime. 17 Juin 1942, Bull. Crime. No. 75.
- Casse. Crime. 2 Janu, 1936, Dp. 1936, 1. 46, note LELIOIR.

أما فى مصر، فلم يذكر قانون الإجراءات الجنائية شيئاً عن قاعدة موافقة ذى الشأن. لكن يمكن تلمس وجود هذه القاعدة من خلال أحكام القضاء[1].

ولتطبيق هذه القاعدة، يجب أن تكون الموافقة:

صريحة لا ضمنية وفى حالة رفض الموافقة الصريحة، فإن ذلك يعنى رفض ذى الشأن، ولذا تعتبر الإجراءات باطلة.

- كما يجب أن تكون هذه الموافقة مكتوبة. فقد نصت المادة ٢/٧٦ من قانون الإجراءات الجنائية الفرنسى، على وجوب أن تكون الموافقة فى شكل إقرار مكتوب بيد ذى الشأن L'Objet d'une de claration écrite de La main de l'interéssé. فإذا كان لا يعرف الكتابة يذكر ذلك فى المحضر وتذكر فيه هذه الموافقة(*).

- كما يجب أن تصدر هذه الموافقة من لدن الشخص ذى الشأن ولا أحد غيره، وفى هذا الخصوص يجب ملاحظة أن المشرع الفرنسى، لم يصرح بأنه عند غياب الشخص الذى يقع عنده التفتيش، فإنه يمكن أن يحل محله شخص آخر يبدى موافقته على إجراء التفتيش[2]. إذ ليس من الممكن قبول الاعتذار بأنه نظراً لغياب المالك فلن يتيسر الحصول على موافقته الشخصية للدخول

---

(١) نقض ٢٣ نوفمبر سنة ١٩٧٥ مجموعة أحكام النقض، س ٢٦ ق، رقم ١٦٣، ص ٧٤٠، نقض ٢٩ يناير سنة ١٩٦٣، مجموعة أحكام النقض، س ١٤ ق، رقم ١٠، ص ٤٣، نقض ١١ نوفمبر سنة ١٩٤٦، مجموعة أحكام النقض، رقم ٢٢١، ص ٢٠٥.

(*) وفى ذلك تقول محكمة النقض الفرنسى: من المقرر أن الموافقة الصريحة من ذى الشأن المزمع إجراء التفتيش فى مسكنه يجب أن تكون مكتوبة، فإذا كان لا يجيد الكتابة إلا جزئياً N'est que partiellement écrit de Sa main، ففى هذه الحالة ينبغى إثبات الاسم، اللقب، السكن، عليها قبل أن يقوم بالتوقيع، وذلك حتى تتحقق المحكمة من استيفاء شروط المادة ٧٦ أ – ج.

Casse. Crime. 28 Janv. 1987, Bull. Crime. No. 48, D. 1987. 258, note AZIBERT.

- وراجع أيضاً: - Note PRADEL, D. 1985, 498.

(2) MIMIN: "art. cité ". No. 26.

في منزله، ولذا استعيض عن ذلك بموافقة الحارس أو بموافقة أبناء هذا الشخص(١).

- وأخيراً يشترط في النظام الأنجلو أمريكي - بالإضافة إلى ما تقدم - أن تكون هذه الموافقة حقيقية، خالية من الخداع والزيف. كما يجب على مأمور الضبط أن يثبت عدم حصول أي نوع من أنواع العنف أو الإكراه على ذي الشأن، لإجباره على إصدار تلك الموافقة(٢).

**- الوضع بالنسبة للموافقة علي التفتيش في نطاق الجريمة المعلوماتية:**

أما بالنسبة لجرائم المعلوماتية، فلا توجد نصوص قانونية مشابهة تتعلق بتفتيش الأوعية المعلوماتية، بناء على موافقة المتهم سواء في مصر أو في القانون المقارن. وبالتالي لا مشاحة في أن هذا الإجراء يمكن تغطيته بالقواعد التقليدية.

بيد أن هذا الإجراء يطرح على بساط البحث سؤالاً منطقياً ساقه الدكتور/ هلالي عبد اللاه - نؤيده فيه - مناطه:

- لماذا يتخلى إنسان عاقل عن الحماية التي يكفلها له القانون؟ وهل يعقل أن يوافق الإنسان على تفتيش شخصه أو منزله بمحض إرادته، أم إن هذه الإرادة كانت ضحية استخدام القوة، أو التهديد أو الخديعة، من جانب رجال الشرطة؟!

ومن هذا المنطلق ينتقد الفقه بشدة هذا الإجراء، خاصة وأن كل حالات الموافقة على التفتيش كانت ناجمة عن عسف رجال الشرطة(٣).

ولذلك ألا ينبغي أن يتطلب الأمر إذناً قضائياً للتفتيش خارج حالات التلبس؟!

---

(1) PARRA et MONTREUIL: op. cit., p. 248.

(2) PAKER et DODGE: op. cit., p. 106 et S.

- CORMICK (Charles): op. cit., p. 274 et S.

(٣) لمزيد من التفصيل حول هذه الانتقادات راجع في الفقه الفرنسي:

- ROBERT (Jacques): "Lés violations de la Liberté individuelle commises par agents Publics et le problème des personalités" These Paris, 1953.
- LANGLOIS (Denis): "Les Dossiers noirs de la police française, Paris Seuil, 1971.

## الفرع الثاني

## إجراء ضبط نظم المعلوماتية

**أوضحنا سابقاً:**

أن الغاية من التفتيش هو ضبط الأدلة المادية التي تفيد في كشف الحقيقة. وعلى ذلك فإن ضبط الأشياء المتعلقة بالجريمة هو الأثر المباشر للتفتيش.

والضبط كإجراء من إجراءات التحقيق هو وضع اليد على الشئ وحبسه والمحافظة عليه لمصلحة التحقيق. والضبط الذى نقصده هنا هو الضبط القضائى Saisie Judiciaire .. الذى يهدف إلى الحصول على دليل لمصلحة التحقيق عن طريق إثبات واقعة معينة(1).

وكذا قد أشرنا سلفاً إلى أن الحاسب الآلى كمحتوى للمعلوماتية يتكون من:

- مكونات مادية Hard Ware.
- مكونات منطقية (معنوية) Soft Ware.

وللحاسب الآلى شبكات اتصال بعدية Net Workd telecommunication (2). حيث يثور تساؤل هام عن مدى إمكانية خضوع مكونات وشبكات المعلوماتية للضبط؟

- فبالنسبة للمكونات المادية للمعلوماتية، لا خلاف فى الرأى فى إمكانية ضبطها.
- وكذلك الحال بالنسبة لشبكات المعلوماتية، إذ يمكن رصد الاتصالات التى تتم خلالها وتسجيل محتوياتها، ومن ثم يمكنه ضبطها.
- بالأضافة إلى إمكانية ضبط الحاسب الشبكى للمعلوماتية بالكامل، لتأكيد الاحتفاظ بالدليل، إذا كان مشغل الجهاز غير متعاون بما فيه الكفاية(3).

---

(1) راجع ما تقدم ص٢٧٨، من الدراسة.

(2) راجع ما تقدم ص ٨١ ، من الدراسة.

(3) بالنسبة للشبكات الكبيرة Large net works فإن هذا الضبط ليس عملياً، لأنه يؤدى إلى التعدى المفرط على حقوق الغير.

- DURHAM (Cole): art. Gté, p. 112.

أما بالنسبة لمكونات المعلوماتية المعنوية فالوضع يختلف، فالأمر ليس بالسهل والمسألة تبدو أكثر تعقيداً وتركيباً - كما ذكر التقرير العام لمؤتمر A.I.D.P(*).

مشكلة لا مادية الحاسب الآلى (وهو الذى يحوى النظم المعلوماتية) The in-corporeality of computer data(١).

فإذا كان التفتيش يتم لمكونات الحاسب المادية كمحتوئ للمعلوماتية، فهل الشئ الذى يتم ضبطه هو هذا الشئ المادى Tangible؟

أم أنه يتضمن كذلك البيانات غير المادية Incorporporeal data؟ وما هو السند القانونى القائم عليه الضبط؟

وفى هذا الشأن تعددت الآراء وتشعبت فى اتجاهات مختلفة(٢):

- حيث ذهب رأى إلى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التى تفيد فى كشف الجريمة وبيان الحقيقة، فإن هذا المفهوم يمتد ليشمل البيانات الالكترونية Electronic Data بمختلف أشكالها.

**تطبيقات تشريعية:**

- **في اليونان:** نجد المادة ٢٥١ من قانون الإجراءات الحالى، تعطى سلطات التحقيق مكنة القيام «بأى شئ Anything يكون ضروريا لجمع وحماية الدليل»(٣).

---

(*) المؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات، والذى عقد فى ريو دى جانيرو بالبرازيل الفترة من ٤-٩ سبتمبر سنة ١٩٩٤.

- XV eme Congrés international de droit Pénal. Rio de Janeiro, Brésil, 4-9 Septembre 1994. Association internationale de droitt Penal, R.I.D.P., 1e et2 e trimestres 1995.

(١) د/ هلالى عبد اللاه أحمد - مرجع سابق - ص ٨١.

(٢) المرجع السابق - ص ٨٢.

(3) VASSILAKI (Irini): art. Cité., p. 371.

ويفسر الفقه اليونانى عبارة «أى شئ Anything» بأنها تشمل ضبط البيانات المخزنة Scizure of data stord أو المعالجة اليكترونياً Processed. ولذلك فإن ضبط البيانات المخزنة فى حاملات البيانات المادية Corporeal data carriers أو فى الذاكرة الداخلية Internal memory لا تسبب أية مشكلة فى اليونان. إذ بمقدور المحقق أن يعطى أمراً للخبير بجمع البيانات؛ التى يمكن أن تكون مقبولة كدليل من المحاكمة الجنائية(*).

- في كندا: نجد نفس الوضع التشريعى فالمادة ٤٨٧ من القانون الجنائى الكندى، تعطى سلطة إصدار إذن لضبط «أى شئ Anything» طالما تتوافر أسس معقولة reason able grounds للاعتقاد to believe بأن الجرم offence ارتكب، أو يشتبه فى ارتكابه، أو أن هناك نية فى أن يستخدم فى ارتكاب الجرم، أو أنه سوف ينتج دليلاً على وقوع الجرم(١).

وحتى الآن فأن هذا النص يقسر بوضوح تام على أنه يسمح يضبط بيانات الحاسب غير المحسوسة Intangille Computer data(**).

- في لوكمسبورج: يشمل الضبط – بصفة عامة – كل الأشياء التى تفيد فى إظهار الحقيقة(٢).

---

(*) كما تجيز المادة ٢٦٠ من قانون الإجراءات اليونانى استخدام القوة العسكرية فى الضبط، فى حالات البنوك أو المؤسسات الخاصة والعامة، من بين المستندات Documents الأخرى التى تكون متعلقة بالجريمة. ولهذا فإن المحققين The investigators بمقدورهم أن يأخذوا البيانات المخزنة فى حاملات البيانات.

(1) Ibid., p. 371.

(**) بالرغم من أنه فى معظم القضايا الحالية، فإن الوعاء المادى المحتوى على البيانات Physical medium containing the data كالقرص Disk هو الذى يتم ضبطه على أية حال.

- Ibid., p. 241.

ولذا جاء فى التقرير العام لمؤتمر A.I.D.P. إنه إذا كان الضبط فى كندا لبيانات الحاسب غير المادية يعتبر قانونياً من الناحية النظرية، إلا أن الوعاء المادى Physical medium الذى يحتوى على البيانات هو الذى يتم ضبطه حالياً بصفة عامة.

يراجع: - DURHAM (Cole): art. Cité. p. 112.

(2) JAEGER (Marc): art. Cité. p. 467.

وفى هذا الخصوص، فإنه يكون من المقبول لدى الفقه هناك أن ضبط مكونات الحاسب، وما يستند عليه من دعائم مادته يتضمن البيانات التى تفترض أنها بداخله.

- في فرنسا: ذهب جانب من الفقه إلى الاعتراف بأن للبرنامج كياناً مادياً ملموساً، يتمثل فى نبضات اليكترونية أو أشارات الكترونية مغناطيسية أو ممغنطة(١).

- وعلى عكس هذا الرأى، هناك من يرى أنه إذا كانت الغاية من التفتيش هى ضبط الأدلة المادية التى تفيد فى كشف الحقيقة، فإن هذا المفهوم المادى لا ينطبق على بيانات الحاسب الآلى غير المحسوسة أو الملموسة، وإزاء هذا القصور التشريعى فإن هذا الرأى يقترح ضرورة أن يضاف إلى هذه الغاية التقليدية للتفتيش عبارة «المواد المعالجة عن طريق الحاسب الآلى أو بيانات الحاسب الآلى».

وبذلك... تصبح الغاية الجديدة من التفتيش بعد هذا التعديل اللغوى الذى يواكب التطور التقنى الحديث، والذى ينبغى أن تنص عليه التشريعات الإجرائية هى:

(البحث عن الأدلة المادية أو أى مادة معالجة بواسطة الحاسب)(٢).

**ونجد ارهاصات هذا الرأي في بعض التشريعات:**

- في هولندا: نلاحظ قريب من ما سبق ذكره، إذ أصدر وزير العدل الهولندى أمره بتشكيل لجنة لدراسة هذا الوضع.

---

(1) SAGROS (Pierre) et MASSE (Michel): "Le droit Péral et L'informatique" en L'informatique et droit Pénal. Journées d'études du 15 Nov. 1980, Publication d'institut de Sciences Criminelle de la facul-té de droit de Poitiers éd. Cujas tom IV, p. 25.

مشار إليه لدى د/ هلالى عبد اللاه أحمد – المرجع السابق – هامش ٣ – ص ٨٣.

(٢) – المرجع السابق – ص ٨٤

وقد اقترحت اللجنة عدداً من الصلاحيات الجديدة، تم صياغتها أساساً طبقاً للقواعد التقليدية للضبط، ولكن مع بعض الاستثناءات المتعلقة بالنواحي غير المادية Intactilc مثل بيانات الحاسب الآلي. وفي هذا الصدد أوصت اللجنة بضرورة إعطاء الشرطة سلطة ضبط هذه النوعية من البيانات من خلال الدعامة المدونة عليها[1].

- في فرنسا: يرى بعض الفقهاء أن النبضات الالكترونية Electronic Impulses أو الاشارات الاليكترونية الممغنطة لا تعد من قبيل الاشياء المحسوسة، وبالتالى لا تعتبر شيئاً مادياً بالمعنى المألوف للكلمة[2]، ولذا لا يمكن ضبطه.

- وطالعنا رأى ثالث لا يقحم نفسه فى هذا السجال الفقهى الدائم بين الرأيين السابقين. حول ما إذا كانت كلمة (شئ) تشمل بيانات الحاسب الآلى من عدمه، وبالتالى يجوز ضبطها أم لا يجوز.

وإنما ينظر إلى الواقع العملى الذى يؤكد أن الضبط لا يتصور، إلا إذا اتخذت بيانات الحاسب الآلى شكلاً مادياً[3].

- في ألمانيا: الإدلة المضبوطة يجب أن تكون أشياء ملموسة (القسم ٩٤ من قانون الإجراءات الجنائية)، وذلك يشمل ليس فقط نظم الحاسب بل أيضاً حاملات البيانات Data Carriés. وهذه البيانات تنقصها الخاصية المادية Corporeal Quality، وبالتالى لا تشكل أشياء يمكن ضبطها

ويتم ضبط البيانات بتصوير الشاشة أو نقلها على حافظة بيانات، ومن ثم يمكن معاملتها ضمن ما يدخل تحت القسم ١٦١ من قانون الإجراءات الجنائية،

---

(1) KASPERSEN (W.K. Henrik): art. Citée. p. 490.

(2) GROZE (H.): "L'Apport du Droit Pénal a la théorie générale du droit de L'informatique", J.C.P. 1988, 333, No. 16.

- GASSIN (R.): "Le Droit Pénal et L'informatique" D. 1982, p. 38.

(٣) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٨٥.

أو بدرجة أقل مقارنة بضبط المطبوعات الخاضعة للقسم ٩٤ من قانون الإجراءات الجنائية(١).

وهكذا ذهب رأى فقهى(٢) – متفقاً مع الفقيه كول دور هام -Cole DURHAM – إلى أن الأشياء المحسوسة Tangible objects فى القانون الألمانى هى التى يمكن ضبطها. ويعنى ذلك بمفهوم المخالفة أن البيانات المجردة Mere Data لا يمكن ضبطها، بينما المطبوعات Printouts أو البيانات المصورة فوتوغرافياً، أو التى تنقل إلى حاملة الاحتفاظ بالبيانات فإنه يمكن ضبطها(٣).

• **في رومانيا:** ينصب الضبط على الدعامة المادية، المدون عليها بيانات الحاسب كالأشرطة المغناطسية أو الأقراص، وليس على الكيان غير المادى Entité en Corporelle(٤).

• **في اليابان:** فإن السجلات الاليكترو – مغناطيسية Electro Magnetic Records تكون غير مرئية فى حد ذاتها Not Visible in Itself ولذلك لا يمكن ضبطها. وبالتالى ينبغى تحويل هذه السجلات الغير مرئية إلى صورة مرئية ومقروءة عن طريق مخرجات الطباعة لمثل هذه السجلات(٥).

بل ان مخرجات الطباعة لمثل هذه السجلات و أى مخرجات أخرى تعد – لدى فقه بعض الدول – من قبيل المستندات المطبوعة التي يمكن ضبطها. ذلك لأن التقدم التقنى قد تجاوز المفهوم التقليدى للمستند الذى يعرفه على أنه مجرد

---

(1) MOHRENSCHLAGER (Manfred): art. Citée, p. 351.

(٢) رأى الدكتور/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٨٥.

(3) DURHAM (Cole): art. Citée, p. 112.

(4) ANTONIU (Georgo): "Les crimes informatiques et d'Autres crimes Dans le domaine de la Technologie informatique en Roumanie" R.I.D.P. 1993, p. 551.

(5) YAMAGUCHI (Atsushi): art,. cité, pp. 448 - 449.

ورقة مكتوبة[1]. وبهذا المفهوم أخذ الفقه في البرازيل[2] والمجر[3] وفنلندا[4]، ومشروع القانون الحالي لدولة شيلي[5].

وقريب من هذا، الفقه السائد في الولايات المتحدة الأمريكية[6]، والمملكة المتحدة[7]، فرغم ان الفقهاء يعترفون أنهم في مجال الحاسب الآلي يتعاملون مع أشكال غير ملموسة من الأدلة Intangible Formes Evidence، إلا أن ذلك لا يشكل مشكلة في تقديرهم، على أساس أنه يمكن ضبط السجلات المعالجة ذاتها، أو المستندات الناتجة عنها، بل وحتى أحياناً ضبط الحاسب الآلي ذاته بافتراض أنه دليل.

- **تأصيل البيان بشأن ضبط مكونات وشبكات المعلوماتية:**

ذهب رأي فقهي[8] – نؤيده – إلى أنه ينبغي أن ننظر إلى طبيعة الكيانات

---

(١) د/ هلالي عبد اللاه أحمد – المرجع السابق – ص ٨٦.

(2) JUNIOR (Joào Marcello de Araujo): "Computer Crimes and other Crimes Against information Technology in Brazil" R.I.D.P. 1993, p. 198.

(3) KERTESZ (Imre) and PUSZTAI (Laszlo): "Computer Crimes and Other Crimes Against Information Technology in Hungary" R.I.D.P. 1993, pp. 385 - 386.

(4) PIHLAJAMAKI (Antti): art. Cité, p. 285.

(5) KUNSEMULLER (Carlos): "Computer Crimes and Other Crimes. Against Information Technology in Chilé r.I.D.P. 1993, p. 358.

(6) WISE (Edward M.) art. Cité. pp. 666 - 668.

وراجع أيضاً:

- DURHAM (Cole): art Cité . p. 112.

حيث يرى أنه لا توجد في الولايات المتحدة الأمريكية صعوبات، في السماح بالتفتيش عن المعلومات في حد ذاتها.

(7) WASIK (Martin): art. Cité - p. 640.

(٨) د/ هلالي عبد اللاه أحمد – المرجع السابق – ص ٨٨.

المنطقية أو البرامج، بمعزل عن طبيعة حق مؤلف أو صاحب هذه الكيانات أو البرامج(*). ومن هذا المنطلق يذهب ذات الرأى إلى أن المدخل لدراسة هذه الطبيعة القانونية هو تحديد مدلول كلمة (المادة) فى العلوم الطبيعية. وفى هذا الصدد نجد أن (المادة) هى كل ما يشغل حيزاً مادياً فى فراغ معين، وأن هذا الحيز يمكن قياسه والتحكم فيه.

وفى ذات السياق تجدر الاشارة إلى أن الكيان المنطقى أو البرنامج يشغل حيزاً مادياً فى ذاكرة الحاسب الآلى، ويمكن قياسه بمقياس معين هو البايت Byte، والكيلوبايت Kilo, Byte، والميجابايتMegabyte (**). وهكذا تقاس سعة أو حجم الذاكرة الداخلية للحاسب، بعدد الحروف التى يمكن تخزينها بها.

---

(*) حيث أن مصدر الخلاف – فى تقدير الدكتور/ هلالى عبد اللاه أحمد – هو الخلط بين أمرين لا يصح الخلط بينهما وهما:

- طبيعة حق صاحب الشئ على الشئ من حيث هو نتاج لفكره من ناحية.
- وطبيعة الشئ فى ذاته من ناحية أخرى.

وأنه لا مشاحة بين الفقهاء فى أن البرامج أو الكيانات المنطقية عمل ذهنى.

فهو خلاصة فكر خبير البرمجة الذى صاغه فى شكل أوامر مرتبة ترتيباً منطقياً موجه إلى الحاسب الآلى، والبرامج بهذا المفهوم تدخل فى نطاق الأحكام الخاصة بحقوق المؤلف.

ومن هذا المنظور عملت معظم التشريعات العقابية فى معظم دول العالم ،على مد مظلة الحماية الجنائية لحقوق المؤلف لتشمل برامج الحاسب الآلى:

* فى فرنسا: القانون رقم ٨٥–٦٥٠ فى ٣ يوليه سنة ١٩٨٥ والذى حل محله قانون الملكية الفكرية رقم ٩٢–٥٩٧، الصادر فى الأول من يوليه سنة ١٩٩٢، والمعدل بالقانون رقم ٩٤–٣٦٠ الصادر فى ١٠ مايو سنة ١٩٩٤.
* فى أمريكا: صدر القانون رقم ٩٦ – ٥١٧ فى ١٢ ديسمبر سنة ١٩٨١.

(**) أصغر وحدة بيانات هى العدد الثنائى أو بت Bit، وهى الاختصار لكلمة الرقم الثنائى Binary-digit – وكل ثمانية بتات تكون بايت Byte، وكل أربع باتيات متلاصقة تكون كلمة. (د/ محمد أحمد فكيرين – مرجع سابق – ص ٣٣).

والكيلوبايت: وحدة من وحدات قياس حجم ذاكرة الحاسب وهى تعنى ١٠٠٠ حرف + ٢٤ حرفاً، أى أن قيمتها الحقيقية ١٠٢٤ حرفاً (الموسوعة الشاملة – مرجع سابق – ص ٢٥٧).

والميجابايت: وحدة من وحدات قياس سعة الذاكرة أو سعة وسائط التخزين المختلفة، وهى تعادل مليون كلمة من كلمات الذاكرة وهو ما يساوى ١٠٢٤ كيلوبايت (الموسوعة الشاملة – ص ٢٩٤).

ومما يعضد الطبيعة المادية لبيانات الحاسب الآلى، أن هذه البيانات تأخذ شكل نبضات الكترونية Impulsions Eléctroniques تمثل الرقمين صفر أو واحد. & 1 . وهى فى هذا تشبه التيار الكهربائى، الذى اعتبره الفقه والقضاء فى فرنسا ومصر من قبيل الأشياء المادية.

ونخلص من ما تقدم إلى أن برامج الحاسب الآلى تنطبق عليها سمات أو خصائص المادة، وبالتالى تدخل فى نطاق الأشياء المادية، يستوى فى ذلك أن تكون برامج نظام أو برامج تطبيقات، إذ لا يوجد اختلاف فى الطبيعة بينهما.. كما ذهبت إلى ذلك محكمة باريس الابتدائية.

Il n'y a pas de Différénce de Nature Entre Les Programmes Produits et Les Programmes d'Exploitation(1).

**البند الأول: ضبط المكونات المادية للمعلوماتية:**

لا يثير ضبط المكونات المادية للمعلوماتية صعوبات فى التنفيذ أو مشكلات فى الفقه المقارن، وبالتالى لا خلاف بين الفقهاء فى إمكانية ضبط الوحدات المعلوماتية الآتية:

١- وحدة المدخلات Input unit بما تشمله من مفردات كلوحة المفاتيح Key Boord، وشاشات اللمس Touch screen، نظم الإدخال المرئى Machine vision sys-tems نظام الإدخال الصوتى Voice input system نظام الفأرة Mouse system نظام القلم الضوئى Light pen system نظام القراءة الضوئية للحروف Optical craracter recognition system نظام قراءة الحروف المغناطيسية Magnetic ink characher readr system ونظام إدخال الأشكال والرسومات.

٢- وحدة الذاكرة الرئيسية Main memory سواء كانت ذاكرة القراءة فقط Read only memory أم كانت ذاكرة للقراءة والكتابة معاً Random access memory.

(1) Dalloz. 1984-77- nate c.le stance.

٣- وحدة الحساب والمنطق Arithmetic and logic unit بما تشمله من دوائر الكترونية ومسجلات.

٤- وحدة التحكم Control unit وما تستعين به من مسجلات وساعات منطقية.

٦- وحدة المخرجات Out unit وما تشمله من وسائط كالشاشة Monitor، الطابعة Printer، الرسم Plotter المصغرات الفيلمية Micro filmed printers.

ومن التطبيقات التشريعية التى تجيز ضبط مكونات المعلوماتية من خلال ما تخوله بعض التنقيات الإجرائية، لسلطة التحقيق من اتخاذ أى إجراء أو أى شئ لازم لجمع أدلة الجريمة والحفاظ عليها(١):

- المادة ٢٥١ من قانون الإجراءات الجنائية اليونانى(٢).
- المادة ٤٨٧ من القانون الجنائى الكندى(٣).
- فى لوكسمبورج: يمكن القول بصفة عامة أن الضبط يشمل:

«كل الأشياء التى تكون مفيدة فى إظهار الحقيقة» بما يتسع ليشمل بالطبع المكونات المادية للحاسب(٤).

على أنه توجد بعض من التشريعات، تنص صراحة على تفتيش مكونات الحاسب الآلى، من ذلك:

- القانون الانجليزى الصادر فى ٢٩ يونيه سنة ١٩٩٠.

والذى طبق اعتبار من ٢٦ أغسطس سنة ١٩٩٠، والذى يطلق عليه قانون إساءة استخدام الحاسب Computer misuse ACT(٥).

---

(١) د/ هلالى عبد اللاه أحمد - مرجع سابق - ص ١٩٩.

(2) VASSILAKI (Irini): art. cité. p. 371.

(3) PIRAGOFF (Danald): art. cité. p. 241.

(4) JAEGER (MARC): art. cité.

(٥) للمزيد من التفصيل يراجع:

- FERBRACHE (CAVID): "Pathology of Computer Visruses", Springer Verlay' London LTD. 1992. p. 233.

وأيضا توجد بعض القوانين التى تقدم قواعد تفصيلية للتفتيش والضبط للمعلوماتية، تطبق على مكونات الحاسب وبياناته فى حالات معينة.

- من ذلك على سبيل المثال.. القسم الفرعى رقم ١٦/١ من قانون المنافسة فى كندا The Competiton ACT.

**البند الثاني: ضبط المكونات المعنوية للمعلوماتية:**

أوضحنا سابقاً - فى الدراسة - أن ضبط المكونات المعنوية للمعلوماتية قد آثار خلافاً كبيراً فى الفقه. فهناك رأى ذهب إلى أنه إذا كانت الغاية من التفتيش هو ضبط الأدلة المادية التى تفيد فى كشف الحقيقة، فإن هذا المفهوم يمتد ليضم البيانات الاليكترونية Electronic data، أو قاعدة البيانات Data Base(*)، بمشتملاتها من ملفات Files وسجلات Record وحقول Fields، وسواء اتخذت برامج نظام System Programs، أو برامج تطبيقات Applications Program Saftware بنوعيها الأساسين(**):

---

(*) هى مجموعة منظمة من الملفات تحتوى على معلومات تختص بموضوع معين. وتحتوى قاعدة البيانات على مجموعة ملفات Files يتفرع كل ملف إلى سجلات Records تتفرع بدورها إلى حقول Fild، وعن طريق هذه التركيبة يمكن بسهولة الوصول إلى الحقول والتعامل معها سواء بإدخال بيانات فيها، أو باسترجاع بيانات منها. (د/ محمد فهمى طلبة وآخرون - مرجع سابق - ص ١٣١).

(**) الملف File هو أحد التراكيب الشهيرة للبيانات على شكل مجموعة من السجلات Records التى تختص بموضوع معين وتعتبر وحدة واحدة. ويمكن تخزينه على ذاكرة دائمة -Permen ant، مثل الأقراص والشرائط المغناطيسية حتى يمكن الرجوع إليه عند الحاجة (المرجع السابق - ص ١٨٥).

- السجل records هو مجموعة من الحقول fields التى تربطها علاقة معينة وتعامل كوحدة واحدة. ويحتوى ملف البيانات على عدد من السجلات المتشابهة فى تركيبها ونوع البيانات Data المخزنة مثل بيانات الطلبة أو بيانات الموظفين... الى أخر هذه البيانات. (المرجع السابق - ص ١٨٥).

- الحقل Fild عبارة عن جزء من السجل Records الذى يمثل مجموعة كاملة من المعلومات عن شئ معين. فمثلاً الملف الخاص بموظفى شركة معينة يمكن أن يحتوى السجل الخاص بكل موظف على الحقول التالية:

-/-

- برامج التطبيقات سابقة التجهيز Ready-made application Packages .
- وبرامج التطبيقت طبقا لاحتياجات User-devclopped application Programs .

**وتطبيقاً لذلك:**

• في اليونان: نجد أن نص المادة ٢٥١ من قانون الإجراءات الحالي تعطي سلطات التحقيق مكنة القيام بأى شئ يكون ضرورياً لجمع وحماية الدليل.

ويفسر الفقه اليوناني عبارة (أى شئ) بأنها تشمل ضبط البيانات المخزنة seizure of data ، أو المعالجة إليكترونياً Processed . ولذلك فإن ضبط البيانات المخزنة في حاملات البيانات المادية Carporeal data carriers ، أو في الذاكرة الداخلية internal memory لا تسبب أية مشكلة في اليونان .

إذ بمقدور – باستطاعة – المحقق أن يعطي أمراً للخبير بجمع البيانات، التي يمكن أن تكون مقبولة كدليل في المحاكمة الجنائية .

---

١- أسم الموظف، ٢- المؤهل، ٣- العنوان، ٤- تاريخ الميلاد، ٥- الوظيفة، ٦- المؤهل العلمي، ٧- الخبرات. وعند البحث مثلا عن بيانات الموظفين الذين يشغلون نفس الوظيفة يتم البحث خلال الحقل رقم (٥) أى أن الحقل يستخدم كوسيلة إلى سجل معين أو مجموعة من السجلات (المرجع السابق – ص١٨٣) .

- برامج النظام : هي البرامج التي تتعلق بتشغيل الحاسب وتشمل نظم التشغيل operating systems والبرامج المساعدة utility programs ، ونظم ادارة قواعد البيانات Data base management systems بالاضافة إلى برامج ترجمة اللغات compilers (المرجع السابق – ص٤٣٥) .

- برامج التطبيقات هي البرامج التي تصمم للقيام بمهام محددة . وهي نوعان :
برامج التطبيقات سابقة التجهيز : وهي تلك التي خططت وكتبت للتحكم في معالجة وحل مهمة خاصة . أما النوع الثاني فهي برامج التطبيقات طبقاً لاحتياجات العمل : وهي تلك البرامج التي يعدها خبير البرمجة خصيصاً لعميل معين، بناء على اتفاق مع هذا العميل وتكون صالحة للوفاء بحاجة منشأته .

- VASSILAKI (Irini) : art. cité. p. 371.

ومن ناحية أخرى تجيز المادة ٢٦٠ من قانون الإجراءات الجنائية اليونانى استخدام القوة القسرية أثناء ضبط المستندات Documents المتعلقة بالجريمة ، فى حالات البنوك أو المؤسسات الخاصة والعامة ، ولهذا فإن المحققين بمقدورهم أن يأخذوا البيانات المخزنة فى حاملات البيانات(١) .

بيد أن المشكلة قد تثور فى الحالات التى تكون فيها البيانات مخزنة فى وحدة معالجة مركزية فى حاسب ضمن شبكة معلومات كبيرة . ففى هذه الحالة فإن صياغة شرط يعطى للمحقق إمكانية ضبط هذا النظام الشبكى بأكمله وعزله عن البيئة المعلوماتية المحيطة به ، لا يعد شرعياً طبقاً لمبدأ التناسب The principle of cammensur abilty ، لما فيه من مساس بحقوق الغير فى النظام محل الضبط(٢) .

- في كندا: تعطى المادة ٤٨٧ من القانون الجنائى الكندى سلطة إصدار إذن لضبط (أى شئ) طالما تتوفر أسس معقولة reasonable grounds للاعتقاد بأن الجرم Offence أرتكب، أو يشتبه فى ارتكابه، أو أن هناك نية فى أن يستخدم فى ارتكاب الجرم، أو أنه سوف ينتج دليلاً على وقوع الجرم(٣)، وحتى الأن فإن هذا النص يفسر بوضوح تام على أنه يسمح بضبط بيانات الحاسب غير المحسوسة Intangible computer data، وبالرغم من أنه فى معظم القضايا الحالية يكون محل الجرم الوعاء المادى المحتوى على البيانات Physical medium containing the data كالقرص Disk يتم ضبطه على أية حال. ولذا جاء فى التقرير العام لمؤتمر .A.I.D.P إنه إذا كان الضبط فى كندا لبيانات الحاسب غير المادية يعتبر قانونياً من الناحية النظرية، إلا أن الوعاء المادى Physical medium الذى يحتوى على البيانات هو الذى يتم ضبطه حالياً بصفة عامة(٤) .

(1) Ibid. p. 371 .

(٢) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص٢٠١ .

(3) PIRAGOFF (Donald): art. cité. p. 241.

(4) DURHAM (Cole): art, cité, p. 112.

• وفي لوكسمبورج، يشمل الضبط بصفة عامة «كل الأشياء التي تفيد في إظهار الحقيقة»[١].

وفي هذا الشأن يكون من المقبول لدى الفقه – هناك – أن ضبط مكونات الحاسب، وما يستند عليه من دعائم مادية يتضمن البيانات التي تفترض أنها بداخله.لكن لا يوجد في قانون الإجراءات الجنائية – بلوكسمبورج – التزام بتقديم ما يحوزه مشغلو نظم المعلومات من عناصر الاقتناع des pièces à conviction، وإنما الأمر بالنسبة لهم – مع ما في ذلك من خطورة إمكانية ضبط نظام الحاسب بأكمله[٢].

وهناك رأي آخر، ينظر إلى الواقع العملي الذي يؤكد أن الضبط لا يتصور، إلا إذا اتخذت بيانات الحاسب الآلي شكلاً مادياً.

• ففي ألمانيا، الأدلة المضبوطة يجب أن تكون أشياء ملموسة (القسم ٩٤ من قانون الإجراءات الجنائية) . وذلك يشمل ليس فقط نظم الحاسب بل أيضاً حاملات البياناتdata carries، وهذه البيانات تنقصها بالضرورة الخاصية المادية Corporeal quality وبالتالي لا تشكل أشياء يمكن ضبطها.

لكن إذا تم طبع هذه البيانات، فان هذه المطبوعات يمكن ضبطها، ويتم ضبط البيانات بتصوير الشاشة أو نقلها على حافظة بيانات، ومن ثم يمكن معاملتها ضمن ما يدخل تحت القسم ١٦١ من قانون الإجراءات الجنائية، أو بدرجة أقل مقارنتها بضبط المطبوعات الخاضعة للقسم ٩٤ من قانون الإجراءات الجنائية[٣].

---

(1) JAEGER (Marc): art, cité, p. 467.

(٢) د/ هلالي عبد اللاه أحمد – المرجع السابق – ص ٢٠٢.

(3) MOHRENSCHLAGER (Manfred): "Computer crimes and other crimes against information technology in Germany" R.I.D.P. 1993, p. 351.

وعندما يتم الضبط فإنه يجب على حائز النظام المعلوماتى إذا طلب منه أى شئ أن يقوم بتسليم هذا الشئ. وفى حالة الرفض يتم اتخاذ الإجراءات القسرية للضبط (القسم ٩٥ من قانون الإجراءات الجنائية). وطالما أن هذا الشخص ليس من الأشخاص الذين يلزمهم القانون بعدم أداء الشهادة. فعليه الالتزام بالتعاون(١).

ويثور تساؤل.. هل هذا الالتزام ينطبق كذلك على إنتاج سجلات البيانات Production of data files وخاصة عملية طبع البيانات؟

بعض المحاكم أكدت على الإلتزام بالتعاون بالنسبة للبنوك.. على سبيل المثال البيانات المرئية للحسابات المخزنة على شرائح ميكرو فيش Micro Fiches(*)، أو حاملة بيانات.

حيث حكمت محكمة أولنبرج الإقليمية Oldenburg Regional Court بأن: المدير الإدارى للشركة التى تكون بياناتها مخزونة فى ذاكرة الحاسب، من واجبه أن يقوم بتقديم هذه البيانات التى فى حوزته - إذا ما طلبت منه - عن طريق طبعها وتسليمها(٢).

وهكذا ذهب جانب من الفقه(٣) - فى مصر - متفقاً مع الفقيه كول دورهام Cole Durham على أن الأشياء المحسوسة Tangible objects فى القانون الألمانى هى التى يمكن ضبطها. ويعنى ذلك أن البيانات المجردة Mere data لا يمكن

---

(١) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٢٠٣.

(*) الميكرو فيش Micro Fiche: عبارة عن لوح صغير طوله ٦ بوصات وعرضه ٤ بوصات. ويمتاز بالقدرة على تخزين ما يقرب من ٢٧٠ صفحة مكتوبة. وبعض الأنواع تخزن ١٠٠٠ صفحة. ويتم ذلك عن طريق التصوير الفوتوجرافى مع التصغير الشديد جداً. (محمد فهمي طلبة وآخرون - مرجع سابق - ص ٣٠٠).

(2) MOHRENSCHLAGER (Manfred): art. Cité, p. 352

(٣) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ٢٠٣.

ضبطها إلا أن المطبوعات Printouts، أو البيانات المصورة فوتوغرافياً، أو التى تُنقل إلى حاملة الاحتفاظ بالبيانات فإنه يمكن ضبطها[1].

- وفي رومانيا: ينصب الضبط على الدعامة المادية المدون عليها بيانات الحاسب كـالأشـرطة المغناطيسـيـة أو الاقـراص، وليس على الكيـان المادى Entité incorporelle[2].

- وفي اليابان: السجلات الاليكترو – مغناطيسية Electro - Magnetic records تكون غـيـر مرئيـة فى حـد ذاتهـا Not visible in itself، ولذلك لا يمكن ضبطها، وبالتالى ينبغى تحويل هذه السجلات غير المرئية إلى صورة مرئية ومـقـروءة عن طريق مـخـرجـات الطبـاعـة لمثل هذه السـجـلات[3]. بـل أن مـخـرجات الطباعة لمثل هذه السجـلات أو أى مـخـرجـات أخـرى تُعد – لدى رأى الفـقـه فى بعض الدول – من قـبـيل المستـندات المطبـوعـة التـى يمكن ضبطهـا. ذلك لأن التـقدم التـقنى قد تجاوز المفـهـوم التـقليدى للمستند الذى يعرفـه على أنه مـجـرد ورقـة مـكتـوبة[4]. وبهـذا المفهـوم أخـذ الفقـه فى دول البرازيل[5]، والمجر[6]، وفنلندا[7]، وشيلى[8].

- وفي الولايات المتحدة الأمريكيـة[9] والمملكة المتحدة[10]، رغم أن الفقه يعترف

---

(1) DURHAM (Cole): art. Cité, p. 112.

(2) ANTONIU (George): art. Cité, p. 551.

(3) YAMAGUCHI (Atsushi): art. cité, p. 448.

(٤) د/ هلالى عبد اللاه أحمد – المرجع السابق – ص ٢٠٣.

(5) JUNIOR (Jodo Marcello de Araujo): "Les crimes informatiques et d'autres crimes dans le domaine de la Technologie informatique en Turquie R.I.D.P. 1993. p. 198.

(6) KERTESZ (Imre), PUSZTAI (Loszlo): art. cité. pp. 385-386.

(7) PIHLAJAMAKI (Antti): art. Cité, p. 285.

(8) KUNSEMULLER (Carlos): art. Cité, p. 258.

(9) WISE (Edward): art Cité. pp. 666 - 668.

(10) WASIK (Martin): art. cité. p. 351.

أنه فى مجال الحاسب الآلى يتعامل مع أشكال غير ملموسة من الأدلة Intan-gible formes evidence، إلا أن ذلك لا يشكل مشكلة فى تقريرهم، على أساس أنه يمكن ضبط السجلات المعالجة ذاتها، أو المستندات الناتجة عنها، بل وحتى أحياناً ضبط الحاسب الآلى ذاته بافتراض أنه دليل، وخاصة فى التحقيقات التى مدارها التبادل غير المشروع للمعلومات.

**البند الثالث: مشكلات عملية في إجراءات ضبط الجرائم المعلوماتية:**

**أولاً: مدي جواز الإطلاع علي المحتويات المعلوماتية:**

تساؤل هام يطرحه البحث، مضمونه هل يجوز لمأمور الضبط القضائى الإطلاع على المحتويات المعلوماتية، التى يتم تنفيذ إجراء التفتيش بشأنها وضبطها؟

- **في التشريع المقارن:**

أجاب القسم ١١٠ من قانون الإجراءات الجنائية الألمانى(١) على هذا التساؤل بما نص عليه: ان سلطة الإطلاع على مطبوعات الحاسب The com-puter printouts، وحاملات البيانات Data carriers الأخرى تقتصر على المدعى العام فقط Only the public prosecutor، ولا يكون لضباط الشرطة الحق فى قراءة البيانات عن طريق تشغيل البرامج أو الوصول إلى البيانات المخزونة(*)، دون إذن من الشخص الذى له حق نقل هذه البيانات. لكن كل ما لهم هو مجرد فحص حاملات البيانات دون استخدام أية مساعدات فنية Tech-nical aids(٢).

(١) د/ هلالى عبد اللاه أحمد – تفتيش نظم الحاسب الآلى – مرجع سابق – ص ٢٠٤.

(*) Police officers to do not have the right to read through data by running programs or accessing files.

(2) MOHRENSCHLAGER (Manfred): art. Cité, p. 351.

**ثانياً: حق المتهم في الصمت:**

قد يحتاج مأمور الضبط القضائي أو المحقق إلى معرفة معلومات معينة من شأنها أن تسهل مهمته في التفتيش والضبط حول بعض الأمور، كقاعدة البيانات Data Base، أو نظام إدارة قواعد البيانات Data Base management system، أو قاموس بيانات Data Dictionary، أو خريطة تدفق البيانات Data flow Die-gram، أو قنوات إرسال البيانات Data Transmission channels، أو الفهرس Di-rectory، أو التصميم التفصيلي للنظام Detailed system design، أو فك الشفرة Decording، أو دائرة حل التشفير Decodes... إلى آخر هذه المسائل المعلوماتية.

فهل يجوز للمتهم أو المشتبه فيه أن يمتنع عن الإدلاء بهذه المعلومات؟

واقع الأمر وصحيحه، أن هذا التساؤل يثير استفهام يتعلق بحق المتهم في الصمت Le droit au silence[1].

فمن المسلم به بداءة أن للمتهم أن يمتنع عن الإجابه، على الأسئلة الموجهة إليه، أو أن يدلي بأية معلومات قد تؤدي إلى إدانته[2]. وحق المتهم في الصمت يوازي في المعنى حق المتهم في السكوت، فكلاهما يقصد به عدم الإساءة للموقف القانوني للمتهم في الواقعة المنسوبة إليه، وضمانه له في الدفاع عن نفسه، إن تعرض لظلم وجود من سلطات الضبط والتحقيق(*).

---

(1) SALVAGE - GERET (P.): "Le Droit de ne pas s'accuser soi-même et la Justice pénale française" Thése Grenoble 1971.

(2) LEIBINGER (R). : "La Protection des droits de l'accusé dans la procédure allemande" R.I.D.P. 1966, p. 22 et s.

(*) لمراجعة المزيد بشأن حق المتهم في السكوت. أنظر:

د/ سليمان عبد المنعم – بطلان الإجراء الجنائي – دار الجامعة الجديدة – ٢٠٠٨، ص ١٧٤.

* المشرع الفرنسي يبدو أكثر صرامة في ضمانه لحق المتهم في الدفاع عن نفسه، من نظيره المصري واللبناني (أنظر المادة ٧٠ من قانون أصول المحاكمات الجزائية اللبناني والمادة

-/-

ويقصد بالحق في الصمت أن الشخص له مطلق الحرية في الكلام أو عدم الكلام، وبناء عليه فإن للمشتبه فيه الحرية في عدم الإجابة على الاسئلة الموجهة إليه من قبل مأمور الضبط القضائى، لأنه غير ملزم بالكلام، ويجب أن يراعى أن رفضه الإجابة وصمته لا يجوز أن يؤخذان قرينة ضده(1). وذلك تطبيقاً للقاعدة العامة التى تقضى بأنه لا يوجد ما يلزم أو يجبر الشخص على الكلام أمام أى جهة أو سلطة، فهذا حق من حقوق الإنسان. وبالتالى لا يجوز إكراه الشخص على الإجابة على الأسئلة الموجهة إليه من المحقق، بل إن للمحقق أن ينبهه إلى أن من حقه ألا يجب إلا بحضور محاميه، وهذا ما أوصى به المؤتمر الدولى السادس لقانون العقوبات المنعقد فى روما سنة ١٩٥٣م، والمؤتمر الدولى الذى نظمته اللجنة الدولية لرجال القانون فى أثينا يونيه ١٩٥٥(*).

--- ١٢٤ إ – جـ مصرى). وقد أجمع الفقه على اعتبار حق المتهم فى السكوت أحد حقوق الدفاع المكفولة للمتهم، ومؤدى أعمال هذا الحق تحذير المتهم من مغبة الأقوال المتسرعة.

مشار إليه لدى: د/ سليمان عبد المنعم – المرجع السابق – ص ١٧٥.

وقد حرص القضاء الفرنسى على تأكيد حق السكوت وعدم الخلط بين:

– قبول المتهم بارادته الكلام.

– وعدم حضور محاميه.

فإذا قبل المتهم الكلام فوراً فعلى المحقق أن يدون أقواله فى محضر، لكن لا يعتبر هذا من قبيل الاستجواب، فيظل المحقق مستمعاً فقط ولا يملك مناقشة المتهم مناقشة تفصيلية، ولا ينبغى أن تتمخض الاسئلة التى يوجهها للمتهم عن دليل إدانه ضده أو تقرير مسئولية.

- Voir: Casse. Crime. 15 mars 1973, Bulltin des arrets de la chambre criminelle de la cour de cassation, No, 134.

(1) للمزيد بشأن صمت المتهم يراجع: د/ سامى صادق الملا – اعتراف المتهم – ط٣– القاهرة – المطبعة العالمية – سنة ١٩٨٦ – ص ١٨٧ وما بعدها.

حيث عرض للصمت الطبيعى والصمت العمدى والحماية القضائية لحق الصمت.

(*) تضمنت توصيات مؤتمر روما سنة ١٩٥٣، «لا يجبر المتهم على الإجابة، ومن باب أولى لا يكره عليها. فهو حر فى اختيار الطريق الذى يسلكه ويراه محققاً لمصلحته».

وفى المؤتمر الدولى الذى نظمته اللجنة الدولية لرجال القانون فى أثينا يونيه ١٩٥٥، قررت لجنة القانون الجنائى أن المتهم يستطيع أن يرفض الإجابة أمام الشرطة وسلطة الاتهام، ويطلب سماعة بواسطة القاضى، ولا يجوز للمحكمة أن تجبره على الكلام.

فإثبات الاتهام على شخص مشتبه فيه، يقع على عاتق سلطة الضبط التى تتولى ضبطه وجمع الأدلة المادية والمعنوية التى تثبت ارتكابه الواقعة، ثم سلطة التحقيق التى أوكل لها القانون مباشرة الدعوى الجنائية وهى الأمينة عليها، وتقديم المتهم بإدلة الاتهام الثابتة فى حقه، وخلال هذه المراحل فإن القانون كفل للمشتبه فيه الدفاع عن نفسه والاستعانة بمحامى للدفاع عنه، واتخاذ كافة الإجراءات لإثبات براءته.

ويستفاد مما سبق أن للمشتبه فيه الحق فى أن يلتزم الصمت إذا شاء، لأن الموقف يخضع لتقديره الخاص، ولا عقاب عليه اذا امتنع عن الإجابة على أى سؤال يوجه إليه، وهذا ما ذهب إليه جمهور فقهاء المسلمين حيث اعتبروا أن الحق فى الصمت حق عام، فالإنسان له الحق فى الإجابة على الاسئلة التى تسألها سلطة التحقيق أو عدم الإجابة والتزام الصمت، وقرروا بناء على ذلك، أنه إذا أقر الشخص على نفسه بارتكاب جريمة ما، فإن من حقه الرجوع عن هذا الاقرار، فإن رجع أى عدل سقط الاقرار، ولا يصح الاستناد إليه فى الحكم بإدانته(١) .

ولم يضع المشرع نصاً صريحاً فى قانون الإجراءات الجنائية يقضى بالتزام المشتبه فيه أو المتهم بالكلام أو بالادلاء بأقواله. كما لم ينص على حقه فى التزام الصمت إذا شاء ذلك. سواء فى مرحلة الاستدلال أو التحقيق الابتدائى، والمشرع بأتخاذه هذا الموقف لم يحسم الأمر فى هذه المسألة، على عكس الحال فى بعض القوانين العربية التى حسمت الأمر بنصها على هذا الحق فى نصوصها القانونية(*) .

---

(١) د/ عبد العزيز محمد محسن – حقوق الإنسان فى الإجراءات الجنائية (فى الفقه الإسلامى) – دار النهضة العربية – سنة ٢٠٠٠ – ص ١٨١.

(*) القانون الكويتى نص فى المادة ٩٨ إ – جـ على حق المتهم فى الامتناع أو رفض الكلام، وعدم الإدلاء بأى تصريح أمام المحقق. القانون السودانى نص المادة ٢١٨/٢ إ – جـ: لا عقاب على المتهم إذا امتنع عن الإجابة على الإسئلة أو أدلى بإجابة كاذبة – القانون الفرنسى م ١١٤/١ إ – جـ تلزم قاضى التحقيق أن ينبه المتهم عند حضوره أمامه لأول مرة، إلى أنه حر فى عدم الادلاء بأى أقرار، ويثبت ذلك التنبيه فى محضر التحقيق.

بينما فى مرحلة المحاكمة نص المشرع على حق المتهم فى التزام الصمت أو الامتناع عن الكلام. حيث تضمنت المادة ٢٧٤ إ – جـ: «لا يجوز استجواب المتهم إلا إذا قبل ذلك».

وتفسير رفض المتهم ا لإجابة على أنه قرينة على الإدانة، يعتبر وسيلة غير مباشرة من وسائل الإكراه. فصمت المتهم لا يعنى أنه مدان، إذ يجب استبعاد الفرض بأن المتهم لا يصمت إلا عندما يجد أن كل وسائل الدفاع عنه مستحيلة، فالصمت قد يكون وليد أسباب عديدة أخرى[1].

كما وأن الاعتراف يلزم أن يقابل دائماً بريبة وحذر، لأن الغالب فى الإنسان العادى أنه لا يذم نفسه، ولا يجرى لسانه مطلقاً بحديث ضد نفسه يجر لذاته عرماً أو عاراً. وعلى هدى هذه الحقيقة الكامنة فى كل إنسان، أقر القانون للمتهم بالحق فى أن يلوز الصمت إذا شاء، إذ لم يضع على عاتقه أى إلتزام بالكلام من قبيل ذلك الذى وضعه على عاتق الشاهد[2].

كما قضت محكمة النقض بأنه من المقرر قانوناً أن للمتهم إذا شاء أن يمتنع عن الإجابة أو عن الاستمرار فيها، ولا يعد هذا الامتناع قرينة ضده، وإذا تكلم فإنما ليبدى دفاعه، ومن حقه دون غيره أن يختار الوقت والطريقة التى يبدى بها هذا الدفاع[3].

وتحرص معظم التشريعات الإجرائية على النص صراحة على حق المتهم فى الصمت[4]:

ومن ذلك الفقرة الأولى من المادة ١١٤ من قانون الإجراءات الجنائية

---

(١) د/ سامى صادق الملا – المرجع السابق – ص ١٨٩.

(٢) د/ رمسيس بهنام – الإجراءات الجنائية تأصيلاً وتحليلاً – جـ٢ – منشأة المعارف – سنة ١٩٧٨ – ص ٣٣٧ وما بعدها.

(٣) نقض ١٧ مايو سنة ١٩٦٠ – مجموعة أحكام النقض س ١١ – رقم ٩٠ – ص ٤٦٧.

(٤) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٢٠٥.

الفرنسى – قبل تعديلها بالقانون ٩٣-٢ الصادر فى ٤ يناير سنة ١٩٩٣ – التى كانت تنص على إلزام قاضى التحقيق بتنبيه المتهم عند حضوره لأول مرة أمامه، إلى إنه حر فى عدم الإدلاء بأى قرار. وأن يشير إلى هذا التنبيه فى محضر التحقيق.

– كما ينص القانون الألمانى فى الفقرتين الثالثة والرابعة من المادة ١٣٦ إ – ج، على التزام كل شخص يقوم بأستجواب المتهم أن يبلغه بأن له الحق فى أن يلتزم الصمت، وأن له الحرية فى أن يدلى بأقواله بالنسبة للوقائع المنسوبة إليه، أو أن يحجم عن ذلك.

– وفى الولايات المتحدة الأمريكية ينص التعديل الخامس من الدستور الفيدرالي، على أنه لا يمكن إجبار أى شخص فى الدعوى الجنائية بأن يشهد ضد نفسه. وفى ذات السياق قضت المحكمة العليا – الأمريكية – بأنه لا يجوز لسلطة الملاحقة الجنائية أن تشير أثناء المحاكمة إلى صمت المدعى عليه أثناء توقيفه لدى الشرطة كدليل إدانه ضده، لأنه لا يمكن منح الشخص حق الصمت، والاستناد فى نفس الوقت إلى هذا الصمت لتحويله إلى دليل إدانه ضده[1].

– وفى بريطانيا وفقاً لقواعد القضاة Judes Rules فإنه يجب على المحقق قبل استجواب المتهم أن يوجه إليه التنبيه التالي[2]:

هل ترغب فى أن تقول شيئاً للإجابة عن هذا الاتهام؟

أنت لست مجبراً على الإجابة إلا إذا رغبت فى ذلك. لكن إذا تكلمت فإن كل ما تقوله يمكن أن يقدم دليلاً ضدك[*].

---

(١) د/ مصطفى العوجى – حقوق الإنسان فى الدعوى الجنائية – بيروت – مؤسسة نوفل – سنة ١٩٨٩ – ص ٥٧٨.

(2) Judges Rules: R.I.P.C. 1973, No. 269.

(*) "Désirez - Vous dire quelque chose en réponse à cette accusation? Vous n'y êtes pas obligé et Vous répondez seulement si Vousle

-/-

كذلك فقد أكد المشاركون فى حلقة دراسات الأمم المتحدة، التى عقدت فى فينا سنة ١٩٦٠ على أن: «المتهم حر فى إبداء رفضه فى تقديم ما لديه من معلومات، وأنه لا يثار أى جدل حول هذه الواقعة عند النظر فى إدانته».

وقد ثبت من خلال هذه الحلقة، أن جميع النظم القانونية تعترف للمتهم بالحق فى الصمت[١].

وإذا انتقلنا من القواعد العامة إلى تخصص الدراسة.. من القواعد الإجرائية التقليدية إلى القواعد الإجرائية الخاصة بالجريمة المعلوماتية، لوجدنا أن مبدأ عدم اتهام الشخص لذاته Self - incrimination Principle يضع حدوداً قوية على المدى الذى يكون فيه المتهم مجبراً على التعاون الفعال Active coopéra-tion فى التحقيقات المتعلقة بجريمته[٢] المعلوماتية[٣]: -

- ففي المجرى المدعى عليه The Person Proceded لا يكون مكرها على إثبات براءته. وفى مستهل استجوابه His interrogation يجب أن يكون متنبهاً إلى أنه غير مجبر على الإدلاء بأى بيان، وبمقدوره أن يرفض الإجابة على الاسئلة أثناء الاستجواب. وذلك يعنى بوضوح أن المشتبه فيه أو المتهم لا يكون مجبراً على طبع سجلات الحاسب Not be obliged to Print out com-puter files أو الإمداد بالأكواد أو كلمات السر Puss Word[٤].

--- désirez. Mais si Vous Parlez, tout ce que vous direz sera consigné et le cas échéant, Pourra servir de Preuve".

(1) Compte rendu en R.S.C. 1960, p. 760. Résolutions du congrés d'Athènes de la commission internationale de Juristes: "Primouté du droit et droits de L'homme". Genève, 1966, p. 30.

(2) DURHAM (Cole): "The Emerging structures of criminal infarmation law, Trcing the contours of a New Paradigm: General Repart for the A.I.D.P. Colloquium, R.I.D.P. 1993, p. 114.

(٣) د/ هلالى عبد اللاه أحمد – مرجع سابق – ص ٢٠٧.

(4) KERTESZ (Imre) & PUSZTAI (Laszlo): "Computer crimes and other crimes against information techology in Hungary" r.I.D.P. 1993. p.366.

بل أن الشاهد Witness يستطيع أن يرفض الشهادة إذا كان ذلك سيؤدى إلى إدانة Incriminate نفسه أو قريب له Kin . وفى مثل هذه الحالات يمكن للشاهد أن يرفض طبع المعلومات التى يتم ا سترجاعها من ذاكرة الحاسب(١).

- وفي بولندا، يقرر مشروع قانون الإجراءات الجنائية The Draft of the code of criminal procedure فى المادة ٦٣ على أن: «المشتبه فيه أو المتهم لا يمكن اكراهه على تقديم مطبوعات الحاسب أو كشف الشفرات السرية Cannot be forced to provide computer print-out, nor display secret codes.

وتحرص الإجراءات الجنائية البولندية - بشدة - على حق المتهم فى رفض أية إيضاحات . وهذا الرفض لا يمكن أن يقابل بأى إجراء قسرى ولا أن يتم تفسيره إضراراً بالمتهم Such refusal cannot be counteracted by any coercive measure nor can it be inter-Preted to the prejudice of the accuse(٢).

- وفي اليابان: مالك Owner الحاسب الذى تم استخدامه ليس عليه التزام التعاون الفعال Obligation to active cooperation، بعبارة أخرى فإن الكشف عن كلمات السرى Passwords أو مخرجات المعلومات Output of information لا يمن أن يرغم على إفشائها(٣).

- وفي الولايات المتحدة الأمريكية: توحي ميزة التعديل الخامس The Fifih Amendment ضد اتهام الذات Self-incrimination لا تسمح بالضبط أو الإفشاء القسرى Forced disclosure للأوراق والكتب الخاصة(*).

---

(1) Ibid.

(2) BUCHALA (Kazimierz): "Computer crimes and other crimes against information Technology in Ploand" R.I.D.P. 1993, p. 515.

(3) YAMAGUCHI (Atsushi): art. cité. p. 448.

(*) المثال التقليدى على ذلك قضية المفكرة Diary . وتخلص وقائع هذه القضية فى أن المدعو BOYETTE كتب فى مذكراته الشخصية بعض التفصيلات عن سلوكه الإجرامى، فى مفكرة يحتفظ بها لنفسه، ثم حدث تفتيش لمنزل هذا الشخص، وتم ضبط هذه المفكرة بما تحويه من
-/-

والتفسير الحالى للتعديل الخامس لا يحول دون مطالبة المشتبه فيه، بأن يعطى السلطات العامة الإذن بالوصول إلى المعلومات التى سوف تعضد تحرياتها. وذلك على أساس أن التعديل الخامس لا يحمى الفرد إلا من الإجبار على أن يدلى بإفادة لها مغزى الشهادة الكلامية Testimonial significance، أى تلك التى تعتمد على مفردات اللغة وتركيبات الجمل دليل غير شهادى - Non Testimonial evidence، أى ليس صيغة كلامية، كما هو الحال فى مطالبته بتقديم عينة من عينات الدم Blood samples. فالمطالبة بتقديم عينة من عينات الدم، هى من الأدلة العلمية المادية. وقياساً على ذلك يمكن مطالبته بأن يسلم قسراً مفتاح الخزانة Strongbox أو مفتاح الشفرة Decoding بالنسبة للمعلومات المخزنة فى نظام الحاسب(١).

وتطبيقاً لذلك أيدت المحكمة العليا - الأمريكية - التكليف بالحضور بطلب شخص تحت التحقيق بتمويل البنوك الأجنبية الإفصاح عن سجلاتها المدونة بها حساباته طرفها. لكن عند التصريح الذى أمر بتوقيعه أشار نظرياً إلى الحاسابت بعبارة **إذا وجدت** Ifany، وبالتالى وجد أن هذه التأشيرة لا تشتمل على توكيد ضمنى حقيقى، بأن تلك الحسابات موجودة، ومن ثم لم تنفذها البنوك.

إلا أن هذا التفسير منتقد فقهاً، لما يثيره من مشاكل، فالتوصل إلى النظام الشفرى لبيانات الحاسب الآلى لا يتم إلا من خلال صيغ كلامية(٢).

---

= وقائع إجرامية. وعندما عرضت القضية على المحكمة، استبعدت هذه المفكرة ولم تستخدمها ضده. لأنها كأى نوع من أنواع الاعتراف اللارادى غير القابل للاستخدام فى ظل التعديل الخامس.

- E.G. United states V. BOYETT, 299. F. 2d, 4th. cir. 1962.

مشار إليه لدى:

- WISE (Edward M.) "Computer crimes and other crimes against information Technology in the united states: R.I.d.P. pp. 666-667.

(1) Ibid., p. 667.

(2) Ibid., p. 667.

**ثالثاً: أجبار المتهم (الشاهد) المعلوماتي علي الادلاء ببيانات:**

**- راي الفقه:**

بشأن مدى إجبار المتهم (الشاهد) على الادلاء ببيانات مخزنة فى محتوى نظم المعلومات (الحاسب الآلى)، وتشكل جريمة، أو مدى امكانية الحصول من المتهم نفسه على رمز الدخول Pass word إلى هذه المعلومات متى كان يعلم بها.

**أ - بخصوص المتهم المعلوماتي:**

الراجح فى الفقه أنه لا يجوز قانوناً إجبار المتهم على طباعة ملفات بيانات مخزنة داخل نظام المعالجة الآلية للمعلومات، أو إلزامه بالكشف عن الشفرات أو كلمات السر الخاصة بالدخول إلى هذه المعلومات، أو إجباره على تقديم الأمر اللازم لوقف الفيروس أو القنبلة المنطقية، لأن القاعدة الأساسية أنه لا يجوز إلزام الشخص بتقديم دليل ضد نفسه، سواء عن طريق الشهادة أو غيرها من عناصر الإثبات. مع مراعاة حق المتهم فى التزام الصمت، دون أن يفسر ذلك على أنه إقرار منه بما هو منسوب إليه من إدلة الإثبات[1]. لكن ذلك لا يمنع من إجبار المتهم على تسليم الشفرة الخاصة بالحاسب الآلى، المخزن فيه البيانات محل الجريمة[2].

**ب- بخصوص الشاهد المعلوماتي:**

الشهادة هى إثبات واقعة معينة من خلال ما يقوله أحد الأشخاص، عما شاهده أو سمعه أو أدركه بحاسة من حواسه عن هذه الواقعة بطريقة مباشرة[3].

والشاهد هو ذلك الشخص الذى يقرر أمام سلطة التحقيق أو القضاء، ما يكون قد رآه أو سمعه أو أدركه على وجه العموم بحواسه[4].

(١) د/ هشام فريد رستم – الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) – مكتبة الالات الحديثة – أسيوط – سنة ١٩٩٤ – ص ٨٢.

(٢) د/ عبد الفتاح بيومى حجازى – مبادئ الاجراءات الجنائية فى جرائم الكمبيوتر والإنترنت – مرجع سابق – ص ٣٦.

(٣) نقض ٥ إبريل سنة ١٩٩٠ – الطعن رقم ٢٤٨٨٠ السنة ٥٩ ق.
ويجوز للمحكمة التعويل على رواية ينقلها شخص عن آخر. نقض ١٧ يونيو ١٩٦٨ – مجموعة أحكام النقض – س ١٩ – رقم ١٤٧، نقض ١٩٧٦/٢/١٥ – س ٢٧ – رقم ٤٣ – ص ٢١٥.

(٤) د/ أحمد فتحى سرور – الوسيط فى قانون الإجراءات الجنائية – مرجع سابق – ط ٧ – سنة ١٩٩٧ – ص ٤٩٨.

ويقصد بسماع الشهود.. السماح لغير أطراف الدعوى الجنائية بالإدلاء بما لديهم من معلومات أمام سلطات التحقيق - والشهادة بهذا المعنى هى الطريق الأكثر شيوعاً فى الإثبات الجنائى(١).

وقد نصت المادة ١١٠ من قانون الإجراءات الجنائية على أنه:

(يسمع قاضى التحقيق شهادة الذين يطلب الخصوم سماعهم ما لم ير عدم الفائدة من سماعهم....).

وقد أثير تساؤل هام حول مدى إجبار الشاهد فى الجريمة المعلوماتية على تقديم دليل فنى يتعلق بهذه الجريمة؟ من ذلك العامل الفنى لأحد الأنظمة المعلوماتية، والذى يقوم لحساب جهات التحقيق بطباعة أو تحليل ذاكرة النظام المعلوماتى ليكشف عن آثار بعض البيانات فيه.

- يختلف الرد على هذا التساؤل، نظراً للاختلاف الذى يطرحه مضمون السؤال بين شاهد عادى وخبير فى الدعوى القائمة.

**- بين الشاهد والخبير:**

يختلف الشاهد عن الخبير فى أن الأول يقدم إلى القاضى معلومات حصل عليها بالملاحظة الحسية، أما الخبير فإنه يقدم إلى القاضى تقارير وآراء توصل إليها بتطبيق قوانين علمية أو أصول فنية(٢).

وقد يجمع الشخص بين صفتى الشاهد والخبير، كطبيب شهد أرتكاب

---

-- وقد قيل فى هذا بأن الشهود هو عيون المحكمة وآذانها، لذا يجب أن تنصب الشهادة على ما رآه الشاهد ببصره أو سمعه بأذنيه أو أدركه لحواسه الآخرى، فلا يجوز أن تتناول الشهادة آراء الشاهد أو معتقداته الشخصية أو تقديره لجسامة الواقعة أو مسئولية المتهم. فتلك أمور تخرج عن دوائر الشهادة.

ويراجع بشأن الشهادة وأنواعها:

- Pisapia, la protection des droitsde l'homme dans la procédure pénale, Rapport Italien, Colloque de 29 au 31 Mars 1978, à vienne.

(١) د/ محمد زكى أبو عامر - الإجراءات الجنائية - دار الجامعة الجديدة - ط ٨ - سنة ٢٠٠٨ - ص ٥٥٨.

وقد أعطى القانون للكافة صلاحية الادلاء بالشهادة إلا فى حالات استثنائية، فيجوز أن يكون الشاهد قريباً للمتهم أو صهراً له أو صديقاً.

(٢) نقض جنائى جلسة ١٩٧٩/٤/٢ - مجموعة أحكام النقض - س ٣٠ - رقم ٩٠ - ص٤٢٦.

جريمة قتل وحاول إسعاف المجني عليه قبل وفاته، فأتيح له بذلك معرفة أسباب الوفاة[1]. أو كرجل حماية مدنية – يعمل فى مجال الحرائق – عاصر اندلاع حريق فطبق الجوانب الفنية فى مكافحة الحرائق – لحين وصول سيارات الأطفاء – فعلم بذلك سبب الحريق ونوعه وبدايته.

**- في تعاون الشاهد:**

أوجبت بعض الدول الأوروبية على الشاهد أن يقوم بأجراء يسمى – إنعاش الذاكرة – Rafraichir leur mémoire وذلك بفحص الأماكن والمستندات التى توجد تحت سيطرته، إذا لم يترتب على ذلك أضرار خطيرة، وذلك كما فى تشريعات دول السويد وفنلندا والنرويج[2].

وفى بعض التشريعات – الانجلو ساكسونية – فإن الالتزام بالتعاون يتسع ليس فقط بمجرد إصدار الأمر بإحضار الشهود، أو لإحضار بعض المستندات، ولكن إلزام الغير بتقديم المساعدة للسلطة القضائية، عن طريق تقديم الأدلة أو المساعدة فى الوصول إليها. ومن ذلك القانون الانجليزى الصادر عام ١٩٨٤ فى شأن البوليس والأدلة الجنائية، ويعطى المحققين الحق فى أن يطلبوا من الغير تمكينهم من الدخول إلى المعلومات المختزنة فى الحاسب الآلى، أو الاطلاع عليها أو قراءتها[3]. وتسمح بعض التشريعات بالاستفادة بالشهود كخبراء أو كمعاونين للقضاء من تلقاء أنفسهم[4].

ولذا فإن الشاهد أو القائم على تشغيل النظام المعلوماتى Opérateur يلتزم بالكشف عن الشفرات أو كلمات السر التى يكون على علم بها، ولا يعفيه من هذا الالتزام سوى التمسك باحترام السر المهنى. ومع ذلك فليس ثمة جزاء جنائى يوقع على الشاهد إذا رفض تقديم المعلومات المطلوبة، إلا اذا وقع ذلك فى مرحلتى التحقيق الابتدائى والمحاكمة[5].

---

(١) د/ جميل عبد الباقى الصغير – أدلة الإثبات الجنائى والتكنولوجيا الحديثة (دراسة مقارنة) دار النهضة العربية – سنة ٢٠٠١ – ص ١٠٦.

(٢) المرجع ذاته.

(٣) المرجع السابق – ص ١٠٧.

(٤) د/ عبد الفتاح بيومى حجازى – المرجع السابق – ص ٣٨.

(٥) د/ جميل عبد الباقى – المرجع السابق – ص ١٠٨.

-/-

- **تعدد وصف الشاهد في النظام المعلوماتي:**

حقيقة الأمر أن ثمة أشخاص أخرين يعدون بمثابة الشهود فى الجريمة المعلوماتية، وهم مقدمى الخدمات الوسيطة فى مجال المعلوماتية والإنترنت، ومن هؤلاء متعهدى الوصول ومتعهدى الإيواء ومسئولى المنتج ومسئولى ناقل المعلومات ومسئولى متعهد الخدمات، وكذلك مورد المعلومات ومؤلف الرسالة، وهؤلاء جميعهم بحكم دورهم فى توصيل - طالب الخدمة - أو المستهلك إلى شبكة الإنترنت[1]. وبيان هذه الفئات:

- **متعهد الوصول:** أى شخص طبيعي أو معنوى يقوم بدور فنى لتوصيل المستخدم (الجمهور) إلى شبكة الأنترنت، وذلك بمقتضى عقود إشتراك تضمن توصيل العميل إلى المواقع التى يريدها.
- **متعهد الإيواء:** هو شخص طبيعى أو معنوى يعرض إيواء صفحات الويب على حساباته الخادمة مقابل أجر. فهو بمثابة مؤجر لمكان على الشبكة للمستأجر (الناشر)، والذى ينشر عليه ما يريد من نصوص أو صور أو ينظم مؤتمرات مناقشة، أو ينشئ روابط معلوماتية مع المواقع الأخرى.
- **المنتج:** يقصد به منتج الخدمة المعلوماتية فى وسائل الاتصال السمعى والبصرى، ولأنه وفقاً للمادة (٩٣-٣) من القانون الفرنسى الصادر فى ٢٩ يوليو ١٩٨٢ إذا ارتكبت جريمة مما نص عليه فى الباب الرابع من القانون الصادر فى يوليو ١٩٨١ بواسطة وسيلة للإتصال السمعى أو البصرى، فإن

---

* ويختلف الوضع فى التشريع الإجرائي المصرى الذى تنص المادة ٢٨٤ منه على أنه:

«إذا أمتنع الشاهد عن أداء اليمين أو عن الاجابة فى غير الأحوال التى يجيز له القانون فيها بذلك، حكم عليه فى مواد المخالفات بغرامة لا تزيد على عشرة جنيهات، وفى مواد الجنح والجنايات بغرامة لا تزيد عن مائتى جنيه».

(معدلة بالقانون رقم ٢٩ لسنة ١٩٨٢ - الجريدة الرسمية، العدد ١٦ الصادر فى ١٩٨٢/٤/٢٢).

وللمزيد بشأن شهادة الشهود يراجع، د/ مأمون محمد سلامة - قانون الإجراءات الجنائية معلقاً عليه بالفقه وأحكام النقض - بدون ناشر - الطبعة الثانية - سنة ٢٠٠٥ - ص ٨٩٨ وما بعدها.

(١) د/ عبد الفتاح بيومى حجازى - المرجع السابق - ص ٣٨ وما بعدها.

مؤلف الرسالة - المادة المعلوماتية - غير المشروعة متى تم تحريك الدعوى الجنائية ضده، فإن منتج الخدمة يعاقب كفاعل أصلى، وذلك دون اشتراط سبق تسجيل المادة المعلوماتية، حتى يقال بأنه مارس حقه فى الرقابة كما هو الحال فى مسئولية متعهد الإيواء(١).

- **ناقل المعلومات (على شبكة الإنترنت)**: يمكن أن يصنف أيضاً كشاهد فى الجريمة المعلوماتية، ويعرف بأنه: «العامل الفنى الذى يقوم بالربط بين الشبكات»، وذلك بمقتضى عقد نقل معلومات - فى هيئة حزم - من جهاز المستخدم إلى الحاسب الخادم لمتعهد الوصول، ثم نقلها من هذا الحاسب الأخير إلى الحاسبات المرتبطة بمواقع الإنترنت أو بمستخدمى الشبكة الآخرين، وذلك من خلال الحاسبات المرّحلة(٢).
- **متعهد الخدمات**: ويمكن اعتباره من قبيل الشهود فى الجريمة المعلوماتية، ويعرف بأنه ناشر الموقع، وهو المسئول الأول عن المعلومات التى تعبر الشبكة، لأنه الوحيد صاحب السلطة الحقيقية فى مراقبة المعلومات التى يجرى بثها.
- **مورد المعلومات**: يعرف بأنه: ذلك الشخص الذى يقوم بتحميل الجهاز أو النظام بالمعلومات التى قام بتأليفها أو جمعها حول موضوع معين، ومن ثم تكون له سيطرة كاملة على المادة المعلوماتية التى تبث عبر الشبكة، فهو الذى يقوم بالاختيار ثم التجميع والتوريد حتى يصل إلى الجمهور فى صورة مادة معلوماتية على الشبكة(٣).

---

(١) د/ مدحت رمضان - جرائم الاعتداء على الاشخاص والأنترنت - دار النهضة العربية - القاهرة - سنة ٢٠٠١ - ص ٥٧.

(٢) د/ جميل عبد الباقى - القانون الجنائى والأنترنت - مرجع سابق - ص١٥٩.
للمزيد من المعرفة بشأن فئات مقدمى الخدمات الوسيطة فى المعلوماتية يراجع: غازى. ج بيتر - ثقافة الكمبيوتر (الوعى والتطبيق والبرمجة) - الطبعة العربية الأولى - مؤسسة الأبحاث اللغوية - نيقوسيا - قبرص - سنة ١٩٨٧.

(٣) المرجع السابق - ص ١٥٣.

وبذلك المعلى يتحقق له السيطرة الكاملة على هذه المعلومات لأنه يملك جمعها من عدمه، ويملك توريدها أو الأمتناع عن ذلك.

• **مؤلف الرسالة:** هو المسئول الأول عن أى معلومات غير مشروعة تتضمنها هذه الرسالة، فإن تضمنت مثلاً عبارات القذف أو السب التى يرسلها أو ينشرها على أحد المؤثرات، فإن مؤلف الرسالة يُسأل جنائياً عن هذه العبارات. كما أنه يمكن سؤاله كشاهد عن المعلومات التى وصلت إليه، من خلال دوره فى خدمة العميل أو المستهلك على الشبكة المعلوماتية[1].

**رابعاً: منع الإطلاع غير المصرح به على نظم المعالجة الألية للبيانات أثناء التفتيش والضبط:**

نصت المادة (٥٢) من قانون الإجراءات الجنائية المصرى، ويقابلاها المادة (٥٨) من قانون الإجراءات الجزائية الاتحادى بدولة الإمارات العربية المتحدة على أنه:

«إذا وجدت فى منزل المتهم أوراق مختومة أو مغلقة بأية طريقة أخرى، فلا يجوز لمأمور الضبط القضائى أن يفضها»[*].

فهل يحظر على مأمورى الضبط القضائى حال قيامهم بالتفتيش لضبط الأدلة فى الجريمة المعلوماتية، الإطلاع على نظام الحماية الآلية للبيانات المخزنة، والمحمية كلياً أو جزئياً ضد الاطلاع؟

وبمعنى أخر هل يُمنع مأمور الضبط القضائى من الإطلاع متى طلبوا ذلك حال قيامهم بالتفتيش[2]:

---

(١) د/ عبد الفتاح بيومى حجازى – المرجع السابق – ص ٤١.

(*) وردت المادة ٥٢ إجراءات جنائية مصرى فى الفصل الرابع دخول المنازل وتفتيشها وتفتيش الاشخاص، من الباب الثانى فى جمع الاستدلالات ورفع الدعوى.

(٢) د/ عبد الفتاح بيومى حجازى – المرجع السابق – ص ٩٥ وما بعدها.

ذهب جانب من الفقه الى أن المادة (٥٢) إ- جـ مصرى، ويقابلها المادة (٥٨) من قانون الإجراءات الجزائية الاتحادى فى دولة الإمارات العربية المتحدة، يحظران على مأمور الضبط القضائى الإطلاع على الأوراق المخترمة أو المغلقة، الموجودة فى منزل المتهم أثناء تفتيشه، ويرى ذات الرأى الرد بالايجاب بشأن منع مأمور الضبط القضائى من الاطلاع على نظام الحماية الآلية للبيانات المخزنة والمحمى كلياً أو جزئياً ضد الاطلاع، إما عن طريق التشفير أو الترميز أو بأى وسيلة فنية أخرى ضد الإختراق. وحجتهم فى ذلك سببين:

**الأول:** أن السبب فى حظر الإطلاع على الأوراق المغلفة والمغلقة والمختومة، هو رغبة صاحبها فى عدم إطلاع الغير عليها، بدليل أنه اتخذ سبل الحماية الممكنة ضد محاولة الاطلاع غير المصرح بها، بدليل إغلاق هذه الأوراق أو تغليفها بأى طريقة.

وذات العلة تتوافر فى البيانات المعالجة آلياً، حيث لا يمكن بدون الحصول على مفتاح الشفرة أو الكود أو رمز المرور Pass Word .. الدخول إلى نظام هذه البيانات، وبذلك يكون صاحب ذلك النظام قد رفض مسبقاً عمليات الأطلاع غير المصرح به، ما لم يكن الراغب فى الاطلاع مصرحاً له عن طريق إعطائه مفتاح المرور إلى هذه البيانات، وذلك لا يتوافر فى حالة مأمور الضبط القضائى القائم بالتفتيش (موضوع الدراسة).

**الثاني:** أن المادة (٥٢) إجراءات جنائية مصرى، (٥٨) إجراءات جزائية إماراتى، يضعان قاعدة عامة بالنسبة للإطلاع على الأسرار، التى حصنها صاحبها ضد الأطلاع غير المصرح به، أيا كان وعاء هذه الأسرار أو البيانات أو المعلومات، يستوى فى ذلك أن يكون وعاءها تقليدياً كالأوراق أو الصور الضوئية أو الفوتوغرافية، أو غير تقليدى عن طريق استعمال الشرائط الممغنطة والأقراص المرنة، وحتى الذاكرات الداخلية للحاسبات، وشبكات المعلومات المحلية والدولية.

فمتى تحقق الغلق فى هذه الوسائط.. فذلك هو (الغلق بأي طريقة) حسب نص المادتين سابقا الذكر.

وعليه أنتهى هذا الرأى إلى أنه يحظر على مأمورى ا لضبط القضائى الأطلاع على هذه البيانات والمعلومات المخزنة، سواء من تلقاء نفسه متى توافرت لديه المقدرة الفنية على ذلك، أو عن طريق أخرين من أهل الخبرة الفنية فى مجال الحاسب الآلى، لمساعدته فى إزالة واختراق الحماية الفنية المقامة حول النظام المعلوماتى محل التفتيش(١).

وفى ذات المسألة ذهب رأى إلى صحة ما سطره هذا الرأى الفقهى(٢)، معللاً أنه يهدف أولاً وأخيراً إلى إيجاد مظلة حماية قانونية، لنظام البيانات المعالجة ألياً، والتى لا يصرح للغير بالإطلاع عليها، ومع محاولة إيجاد هذه الحماية فى ضوء المتوافر من نصوص قانون العقوبات. ويضيف أنه قبل التسليم بصحة الرأى الفقهى – المؤيد لحظر الإطلاع – علنيا مراعاة الآتى:

أولا: أن المستوى الثقافى المتواضع فى الوقت الحالى لأجهزة العدالة، سواء تمثلت فى رجال الشرطة والأمن أو جهات التحقيق أو المحاكم، يجعل مسألة الإطلاع غير مسموح به، والمثارة فى هذا الفرض مجرد تصور نظرى، لأن مأمور الضبط أو رجل التحقيق ليست لديه المقدرة الفنية أو التفتيش على عملية الدخول إلى شبكة البيانات المعالجة ألياً والإطلاع عليها، سيما لو كان الأمر يتصف بالسرية، ومن ثم سيكون هناك احتياطات أمنية متمثلة فى الأكواد السرية وعمليات التشفير والترميز(٣).

---

(١) للمزيد بشأن مراجعة عرض هذا الرأى والحجج التى استند إليها، د/ هشالم محمد فريد رستم – أصول التحقيق الجنائى والفنى واقتراح بإنشاء آلية عربية موحدة للتدريب التخصص – بحث مقدم لمؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات – سنة ٢٠٠٠ – ص ٣٥ وما بعدها.

(٢) د/ عبد الفتاح بيومى حجازى – المرجع السابق – ص ص ٩٧ – ٩٨.

(٣) فى وسائل الحماية من الأرهاب الإليكترونى يراجع: ستيفن فليسون – (الجريمة الإليكترونية فى القرن الـ ٢١) – بحث مترجم بمعرفة أ/ أمنة على يوسف – مركز البحوث والدراسات بشرطة دبى – العدد ١٠٠ – ابريل ٢٠٠٠.

ثانيا: أن عمليات الاختراق أو القرصنة الإليكترونية ليست قاصرة داخل المؤسسة أو داخل الدولة، بل قد يكون المتدخل من خارج حدود الدولة، ذلك أن التكنولوجيا وثورة الاتصالات قد ألغت ما يسمى بالحدود الجغرافية، وأصبحت عملية الاختراق الإليكترونى تتجه لخدمة المصالح السياسية والاقتصادية بين الدول. وذلك يتطلب ضرورة تفعيل التعاون الدولى فى مجال مكافحة الجريمة المعلوماتية.

ثالثا: أن الرأى الفقهى المذكور اجتهد فى ضوء ما هو معروض من نصوص قانون العقوبات السارى، وذلك لعدم وجود قواعد عقابية تراعى الطبيعة الخاصة لجريمة المعلومات، ولذلك يتعين أن يؤخذ بعين الاعتبار وضع تشريع عقابى موضوعى وإجرائى متكامل لمواجهة الجريمة المعلوماتية، يراعى مبادئ المشروعية والمبادئ الدستورية، مع التحلل من القواعد التقليدية فى قانون العقوبات وقانون الإجراءات الجنائية، والتى قد تكون غالباً قاصرة عن مواجهة الجريمة المعلوماتية.

- **رأي الباحث:**

نتفق مع جانب الفقه الذى يرى عدم جواز إطلاع مأمورى الضبط القضائى على أنظمة البيانات المعالجة ألياً متى كانت فى نطاق حماية ألية، لا يمكن بدون الحصول على رمز المرور Pass Word الدخول إلى نظام هذه البيانات. أما ان كانت متاحة ويمكن الاطلاع عليها فتخضع لإجراء التفتيش.

- وأن القياس بين الأوراق المختومة أو المغلقة، ونظام البيانات المعالجة آلياً، قياس يحمد عليه واضعه، لأنه يضفي المرونة على القواعد التقليدية الإجرائية، فى مواجهة الجرائم الافتراضية التى تمخضت عن تكنولوجيا القرن الحادى والعشرين.

- وأن وضع قاعدة عامة بناء على نص القانون (مغلقة بأية طريقة

أخرى)، سواء فى المادة (٥٢) إ –جنائية مصرى، أو (٥٨) إ – جزائية إماراتى، يمثل حماية تشريعية لحقوق الإنسان – المتهم حال القيام بإجراء التفتيش بحقه – وهى قاعدة صالحة للتطبيق لحماية الاسرار والبيانات والمعلومات سواء أكانت فى وعاء تقليدى كالأوراق أو الصور، أو فى وعاء غير تقليدى كالشرائط اللمغنطة والأقراص المرنة والذاكرة الداخلية للحاسب وشبكات المعلومات (محلية ودولية).

مع ملاحظة أن المشرع لم يترك الأمور على أطلاقها هكذا، بل أنه لمراعاة المصلحة العامة وحقوق المجتمع، نظم تعامل مأمور الضبط القضائى مع هذه الأشياء المختومة أو المغلقة(*).

كما نتفق مع الرأى المؤيد لما ذهب إليه جانب الفقه[1]، فى أن الهدف من الاجتهاد ايجاد مظلة حماية قانونية لنظام البيانات المعالجة آلياً والتى لا يصرح للغير بالإطلاع عليها، ومع محاولة إيجاد هذه الحماية فى ضوء المتوافر من نصوص إجرائية تقليدية.

---

(*) يراجع فى ذلك: نص المادة (٥٣) إ – جـ مصرى: (لمأمورى الضبط القضائى أن يضعوا الأختام على الأماكن التى بها أثار أو أشياء تفيد فى كشف الحقيقة... ويجب عليهم إخطار النيابة العامة بذلك فى الحال، وعلى النيابة العامة إذا ما رأت ضرورة ذلك الإجراء أن ترفع الأمر إلى القاضى الجزئى إقراره). معدلة بالمرسوم بقانون رقم ٣٥٣ لسنة ١٩٥٢ – الوقائع المصرية – عدد رقم ١٦٣ مكرر – صادر فى ٢٥ ديسمبر سنة ١٩٥٢.

فلو أن نظام البيانات المعالجة آلياً ومتوفر له سبل حماية آلية، يفيد فى كشف الحقيقة، يكون على مأمور الضبط القاضى التحفظ على المكان الذى به واخطار النيابة بذلك لأعمال شأنها.

نص المادة (٥٥) إ – جـ مصرى: (لمأمورى الضبط القضائى أن يضبطوا الأوراق الأسلحة وكل ما يحتمل أن يكون قد استعمل فى ارتكاب الجريمة... وكل ما يفيد فى كشف الحقيقة ...........................................................................)

فلو أن الفقه ذهب فى رأى إلى عدم جواز إطلاع مأمور الضبط القضائى على نظم البيانات المعالجة آلياً (ومغلقة).. إلا أن المشرع نص لهم على أن يضبوطها (قياساً على ضبط الأوراق...) شريطة أن تفيد فى كشف الحقيقة. فتدخل نظم البيانات المعالجة آلياً وذات حماية ألية فى المعنى العام لنص المادة والذى مؤداه ضبط كل ما يفيد فى كشف الحقيقة.

(١) د/ عبد الفتاح بيومى حجازى – المرجع السابق – ص ٩٧.

ولكن نختلف معه فيما ذهب إليه من مراعاة بعض الأمور فى سبيلنا إلى تأييد عدم جواز إطلاع مأمور الضبط على نظم البيانات المعالجة ألياً، وذلك لما يلى:

**أولاً: المستوي الثقافي المتواضع في الوقت الحالي لرجال الضبط والتحقيق، يجعل مسألة الإطلاع غير مسموح به.**

الرد: هذا الأمر في غير محله. لأن مسألة الخلاف فى الموضوع هى هل يحظر على مأمور الضبط القضائى الإطلاع على نظام البيانات المعالجة آلية، والمحمى كلياً أو جزئياً ضد الاطلاع؟ أم يسمح له بالإطلاع ويصرح بذلك؟

فلم تتعرض الآراء للقدرة الفنية للقائم بالإجراء، فهب أن مأمور الضبط القضائى لديه القدرة الفنية التى تمكنه من الدخول إلى شبكة البيانات المعالجة آلياً والإطلاع عليها، فهل هذا الإجراء يكون صحيحاً ومطابقاً للقانون.

**ثانياً: أن عمليات الاختراق أو القرصنة الإلكترونية ليست قاصرة داخل المؤسسة أو داخل الدولة، بل قد يكون المتدخل من خارج حدود الدولة.**

الرد: وهذا الأمر خارج نطاق المسألة التى مفادها الإطلاع غير المصرح به لمأمور الضبط القضائى على الأوراق المخترمة أو المغلقة، والذى يمتد إلى نظام المعالجة الآلية للبيانات والمحمى كلياً أو جزئياً.

على الرغم من أهمية ما سطره فى نهاية الملحوظة من ضرورة تفعيل التعاون الدولى فى مجال مكافحة الجريمة المعلوماتية.

فأساس الأمر اجتهاد فقهى لبسط حماية القواعد القانونية الإجرائية على النظام المعلوماتى، وذلك يبعد كثيراً عن عمليات الاختراق الإليكترونى، الذى يعد اعتداء صريح على النظم المعلوماتية.

**ثالثاً: أن اجتهاد الرأي الفقهي جاء في ضوء ما هو معروض من نصوص قانون العقوبات الساري.**

الرد: إن ما نحن بصدده اجتهاد فقهى، لتفسير نصوص قانون الإجراءات الجنائية، وأضفاء المرونة عى القواعد الإجرائية التقليدية بالقياس على ما نصت عليه

من نصوص آمره تتضمن مواد قانونية، يمكن تطبيقها على مستحدثات العصر من أفعال وأعمال.

**خامساً: إجراء تحريز الاقراص المرنة المضبوطة في الجريمة المعلوماتية:**

فى نطاق قيام مأمور الضبط بتنفيذ ما نص عليه القانون من تحريز المضبوطات(*)، أن يراعى عند تحريز أقراص الحاسب الآلى وخاصة الأقراص المرنة Floppy disks مجموعة من القواعد الهامة للمحافظة عليها من التلف أو تلاشى البيانات المسجلة عليها، حيث أنه بذلك يحافظ على الدليل المستمد من هذه المضبوطات، ونجمل هذه القواعد فيما يلى:

- عدم ثنى القرص. لأن ذلك قد يؤدى إلى تلفه وفقدان البيانات المسجلة عليه.
- عدم تعريض القرص لدرجات الحرارة العالية أو المنخفضة. وحدود درجات الحرارة المسموح بها تتراوح ما بين ١٠ درجات – ٥٢ درجة مئوية. لأن تمدد أو انكماش الأقراص يؤدى إلى تلفها وفقد ما عليها من بيانات.
- عدم تعريض القرص للأتربة وذرات الغبار والدخان. لأن ذلك يؤثر على السطح المغناطيسى مما يجعله غير قابل للقراءة أو الكتابة. ولذا من الأفضل أن يوضع فى غلافة البلاستيكى الذى يحافظ عليه ويغطى أجزائه.
- عدم تعريض الأقراص للمجالات المغناطيسية، بعدم وضعها على الأجهزة أو السطوح المعدنية حتى لا تفقد ما عليها، لأن التسجيل على الأسطوانة أو القرص يتم مغناطيسياً.
- يجب حمل الأسطوانة أو القرص من الركن العلوى عند علامة الشركة، وإدخالها أو أخراجها من مشغل الاسطوانات أو الأقراص برفق، للمحافظة على القرص والمشغل.

---

(*) ورد فى المادة ٢٤ من قانون الإجراءات الجنائية رقم ١٥٠ لسنة ١٩٥٠ أنه:
«يجب على مأمورى الضبط القضائى أن يقبلوا التبليغات والشكاوى التى ترد اليهم بشأن الجرائم.....، وعليهم أن يتخذوا جميع الوسائل التحفظية اللازمة للمحافظة على أدلة الجريمة.....، وترسل المحاضر إلى النيابة العامة مع الأوراق والأشياء المضبوطة».

- عدم الضغط على القرص بوضع أشياء ثقيلة عليه، مثل وضع احراز أخرى عليه، أو وضعه مع احراز أخرى متفاوته فى الحجم.
- عدم كتابة بيانات على اللاصقة الورقية للمستخدم بعد لصقها على القرص، لأن الضغط بالقلم قد يفسد سطح القرص، وان كان لابد تكون الكتابة على العلبة البلاستيكية الخارجية.

**البند الرابع: نماذج تطبيقية لجرائم مرتبطة بتكنولوجيا المعلومات:**

سبق أن أوضحنا كيف أثرت ثورة تكنولوجيا المعلومات فى هذا النوع من الجرائم، وكيف تهيأت الفرصة لمرتكبيها لاصطياد ضحاياهم من دول أخرى، حتى إن بعض الشبكات الإجرامية قد اتخذت شكل الجريمة المنظمة عبر الوطنية، من حيث تعدد أعضائها، وتوافقهم الفكرى، وكيفية تجميع وتوزيع عائدات أنشطتهم غير المشروعة وتواجدهم فى عدة دول، ولا تجمع بينهم سوى بعض المواقع على شبكة نظم المعلومات (الإنترنت).

ونعرض فيما يلى لبعض نماذج من هذا النوع من الجرائم(١):

**القضية الأولي: تزوير البطاقات «جزئياً» بتلقين الشريط الممغنط لبيانات مختلفة:**

تبلغ من مسئولى أحد محال تجارة الأجهزة الإلكترونية بالقاهرة بالاشتباه فى سلامة بيانات بطاقة دفع اليكترونية، تقدم بها أحد الأشخاص للمحل لشراء هاتفى محمول.. بالانتقال الفورى للمحل المشار إليه، تبين وجود أحد الأشخاص يدعى أ. أ. م. مواليد ١٩٨٣م طالب بالجامعة ومقيم بالإسكندرية وبحوزته بطاقتا دفع إليكترونى تحملان بياناته، شارعاً فى شراء هاتفين محمولين قيمتهما ٧٠٠٠ سبعة آلاف جنيه، وقد ارتاب موظف المحل فى أمره لسابقة تردده على المحل منذ أسبوعين وشرائه جهازى تليفون محمول من ذات

---

(١) لواء/ نجاح محمد فوزى – وعى المواطن العربى تجاه جرائم الاحتيال – مرجع سابق – ص ١٧٨ وما بعدها.

الماركة بموجب بطاقة أخرى، «كان قد أفاد البنك بعد انصرافه أن العملية مرفوضة»، ولدى أصطحاب المذكور والبطاقتين للإدارة تبين أن برفقته آخرين هما كل من م. ى. أ مواليد ١٩٨٢م، م.م.ف. مواليد ١٩٨٤م وهما طالبان فى الجامعة ويقيمان بالإسكندرية.

وبفحص البطاقتين المضبوطتين فنياً، تبين أنهما مزورتان عن طرق تلقين الشريط الممغنط ببيانات بطاقتين لأجانب آخرين، وبمواجهة المتهم المذكور اعترف باستعماله للبطاقات المزورة، التى يتم إعدادها وتزويرها بمعرفة مرافقه م.ى. أ.وبمواجهة الأخير اعترف بقيامه بتزوير البطاقات باستخدام وحدة تكوين البيانات الممغنطة الكترونياً، وجهاز حاسب آلى بمسكنه بمدينة الإسكندرية.

بعد تقنين الإجراءات تم استهداف مساكن المتهمين الثلاثة حيث عثر بمسكن المتهم الأول م.ى.أ على ما يلى:

١- جهازى حاسب آلى وبعض الإسطوانات المدمجة - CD.

٢- جهاز قراءة وتكويد البيانات الخاصة بالبطاقات الممغنطة.

٣- عشرين بطاقة بلاستيك ممغنطة خام معدة للتزوير.

٤- ست بطاقات ائتمانية بأنواع مختلفة، بعضها باسم المتهمين والبعض الآخر بأسماء أجنبية.

٥- خمسة وثلاثين إشعار خصم اليكترونى لمشتريات تم إجراؤها، قيمتها ٩٨,٧٩٩ ألف جنيهاً باستخدام بطاقات مزورة.

٦- صور ضوئية لبطاقات دفع إليكترونى، منسوبة لبعض البنوك الأجنبية.

٧- وبفحص جهازى الحاسب الآلى والأسطوانة تبين تحميلهم لملفات تحوى:

أ - أعداد كبيرة الأرقام لبطاقات ائتمان منسوبة لبنوك فى دول مختلفة، تطابقت أعداد منها مع ذات الأرقام المبينة بإشعارات الخصم والبطاقات المضبوطة بحوزة المتهمين.

ب- صوراً لوجهى بطاقات ماستر كارد وأميركان اكسبريس، موضحاً عليها عناصر البطاقات ووسائل تأمينها.

بطوير مناقشة المتهمين قرر المتهم الأخير، بتحصله على أرقام البطاقات من أحد الأجانب من محترفي هذا النشاط، من خلال أحد مواقع الدردشة على شبكة الإنترنت، وقام بشراء وحدة قراءة وتكويد البطاقات الممغنطة من أحد المواقع التجارية على الشبكة المشار إليها، التي وصلته عن طريق البريد DHL بعد أن حول قيمتها بواسطة شركة ويسترن يونيون. وتحرر بشأن الواقعة المحضر اللازم وتم عرض المتهمين والمضبوطات على النيابة العامة للتصيرف.

**القضية الثاني: اشتباه في عمليات شراء:**

تبلغ من أحد البنوك الوطنية الكبرى باشتباه مركز البطاقات في سلامة عدة عمليات شراء، تمت بأحد محال المفروشات بأحد المراكز التجارية الكبرى بالقاهرة، بلغ إجمالها سبعة آلاف وستمائة جنيه، اتضح من الفحص السريع واللاحق بالتنسيق مع مركز البطاقات بالبنك، أن تلك العمليات قد تمت باستخدام بطاقة ائتمانية منسوبة لمؤسسة ميريل لينش بالولايات المتحدة الأمريكية، وأن صابحها الأمريكي الجنسية لم يسبق له التردد على مصر ومازالت البطاقة بحوزته.

**وفي كمين أعد سلفاً لهذا الغرض تم ضبط كل من:**

- هـ. أ. ع محام ومقيم بالجيزة.
- أ. م. س صاحب محل قطع غيار سيارات ومقيم بالقاهرة، حال ترددها على محل المفروشات بالمركز التجاري، وضبط مع الأول كمية من إشعارات الخصم خاصة بذات المحل وثلاث بطاقات باسم المتهم صادرة من بنك مصر، وبفحصهما فنياً بالإدارة تبين أن شريطهما الممغنط ملقن ببيانات بطاقة أخرى منسوبة للمؤسسة الأمريكية المشار إليها.

بمواجهة المتهمين أنكر الثاني صلته بالواقعة، بينما اعترف الأول بحيازته للمضبوطات، وسابقة تردده على ذات المحل ومحال أخرى لشراء مفروشات وأجهزة وأثاث بموجب تلك البطاقات المزورة، وأضاف أنه يتحصل عليها من

آخر يدعى م.م.ع، حيث أشارت التحريات اللاحقة إلى أن الأخير طالب بكلية الطب ومقيم بالهرم، وأنه استغل اتقانه فى التعامل مع الحاسب الآلى وشبكة الانترنت فى الولوج إلى العديد من مواقع القرصنة على شبكة الانترنت، وسرقة بيانات البطاقات الائتمانية الخاصة بالغير، وتلقيدها لبطاقات مزورة أو خاصة بآخرين لاستخدامها فى تمويل عمليات شراء من المحال التجارية داخل مصر.

عقب استئذان النيابة العامة تم ضبط الأخير وعثر بمسكنه على ما يلى:

١- جهازى حاسب آلى أحدهما نقال.

٢- كمية من إشعارات الخصم خاصة ببطاقات ائتمانية عديدة وكذا العديد من قسائم تحويل الأموال المنسوبة لمؤسسة «ويسترن يونيون» تفيد تحويل مبالغ مالية لآخرين بالخارج.

٣- جهاز قراءة وتكويد البيانات على الأشرطة الممغنطة للبطاقات.

٤- مجموعة من بطاقات الخصم باسم المتهم وملقنة لبيانات بطاقات أخرى.

٥- مجموعة من الأقراص المدمجة CDs.

٦- أربعة هواتف محمولة حديثة لماركات مختلفة وسيارة ماركة أوبل حديثة، من متحصلات النشاط الإجرامى للمتهم.

وبتفتيش مسكن المتهم الأول عثر بحوزته على كميات من الأجهزة والسلع المعمرة، والأثاث الحديث واللوحات الزيتية الثمينة تم شراؤها حديثاً بموجب البطاقات المزورة، وكذا سيارة ماركة ستروين حديثة من متحصلات النشاط أيضاً.

وبفحص جهازى الحاسب الآلى والأقراص المدمجة تبين أنها تحوى:

١- أعداداً كبيرة من الملفات، بعضها يحوى أعداداً هائلة من أرقام بطاقات الدفع الإلكترونى، المنسوبة لبنوك فى العديد من دول العالم.

٢- أعداداً كبيرة من الرسائل داخل صندوق البريد الإلكترونى الخاص بالمتهم، تفيد تبادله لكميات هائلة من أرقام البطاقات، المنسوبة للعديد من البنوك والمؤسسات المالية، فى دول العالم المختلفة منذ عدة سنوات.

٣- أمكن حصر ما يزيد على ٥٠,٠٠٠ خمسين ألف رقم بطاقة فيزا، وأعداد كبيرة منها مقترن بالأرقام السرية الخاصة بأصحابها.

٤- مجموعة كبيرة من برامج وأدوات القرصنة على شبكة الانترنت، مما تساعد على اختراق المواقع والشبكات، من خلال استغلال نقاط الضعف في أنظمة التشغيل في أجهزة الشركات.

٥- مجموعة من الملفات تفيد ارتباط المتهم بعلاقات واسعة مع آخرين، من خلال غرف الدردشة، والمجموعات الإخبارية على شبكة الانترنت.

وبتطوير مناقشة المتهم الأخيرم.أ.ع. اعترف بنشاطه في تزوير بطاقات الدفع الاليكتروني، باستخدام وحدة التكويد المضبوطة بحوزته، وأضاف أنه يقوم بدور الوساطة في بيع وتداول أرقام وبيانات بطاقات الدفع الإلكتروني، الخاصة بالبنوك والمؤسسات المالية على الشبكة الدولية، نظير مبلغ يتراوح بين اثنين إلى خمسة دولارات أمريكية للبطاقة الواحدة، يتم إيداعه في حساب خاص به، قام بفتحه لهذا الغرض على موقع إحدى المؤسسات المالية بالشبكة الدولية، ويقوم بصرف ما يحتاج إليه من مبالغ من ذلك الحساب، باستخدام بطاقة صرف نقدي E-Gold من آلات السحب النقدي المنتشرة داخل مصر أو خارجها.

تم إخطار المنظمة الدولية للشرطة الجنائية (الانتربول) وكذا مؤسستي فيزا وماستر كارد بأرقام البطاقات، وأسماء المواقع التي يرتادها المتهم للتعامل معها فنياً ومصرفياً.

باشرت النيابة العامة التحقيق وأمرت بحبس المتهمين الثلاثة احتياطياً على ذمة القضية، إلى أن تمت إحالتها لمحكمة جنايات القاهرة، التي أصدرت حكمها بالسجن المشدد على المتهم الأخيرم.أ.ع لمدة ست سنوات، والمتهم الأول بالسجن لمدة عامين بينما تم استبعاد المتهم الثاني من الاتهام.

**القضية الثالثة: تصيد:**

سرقة بيانات بطاقات الدفع الإلكتروني بطريق التصيد Phishing، واستخدامه في تمويل عمليات شراء أو سحب أو تحويلات نقدية.

تبلغ من المنظمة الدولية للشرطة الجنائية Interpol، بما ورد من انتربول واشنطن بتعرض شركة ويسترن يونيون «وهى مؤسسة مالية متخصصة فى تحويل الأموال بين دول العالم المختلفة، للاحتيال وذلك من مواطنين فى عدة دول من بينها مصر والأردن والإمارات العربية المتحدة، تونس، تركيا، رومانيا، وقاموا بإجراء تحويلات نقدية بواسطة خدمة تحويل الأموال التى تقدمها الشركة من خلال موقعها على شبكة الانترنت، باستخدام أرقام بطاقات ائتمان تحصل عليها المتهمون من خلال رسائل بريد اليكترونية خادعة.. وقد أرفق ببلاغ انتربول واشنطن عدة كشوف، تتضمن المعلومات الفنية للعمليات الاحتيالية التى تم إجراؤها بالأسلوب المشار إليه.

بمراجعة إدارة العمليات بشركة ويسترن يونيون بالقاهرة، أمكن تحديد بيانات عدد ثلاث مئة وستين عملية تحويل أموال لفروع الشركة بمصر بلغ إجمالها مئتين وثلاثين ألف دولار أمريكى، كل تحويل يقترب من الألف دولار تقريباً، وتم صرفهم بالفعل بمعرفة العديد من الأشخاص مقيمين فى إحدى عشرة محافظة.

وقد أسفرت عمليات التحريات الميدانية، المصحوبة بنتائج الفحص الفنى والتتبع الإليكترونى العكسى لتلك العمليات، على أن وراء كل تلك الحالات مجموعة من العناصر النشطة، من محترفى القرصنة على شبكة الانترنت أمكن تحديدهم.

بعد تقنين الإجراءات تم ضبط سبعة أفراد منهم بمحافظة القاهرة، والدقهلية والإسكندرية وضبط بحوزة بعضهم أجهزة الحاسب الآلى التى استخدمت فى إجراء تلك العمليات ومجموعة من بطاقات الدفع الإلكترونى «بطاقات خصم من نوع E-gold وإخطارات صادرة عن بعض شركات البريد» بوصول طرود من الخارج باسم أحد المتهمين عن عمليات تمت باستخدام بطاقات ائتمانية خاصة بأجانب، وكذا كمية كبيرة من الكتب والمراجع الأجنبية وبرامج الحاسب الآلى

الثميدة، التى قام المتهم نفسه بشرائها من العديد من المواقع على شبكة الانترنت، باستخدام أرقام بطاقات ائتمانية خاصة بأجانب.

وبفحص أجهزة الحاسب الآلى المضبوطة تبين أن كلا منها محمل بما يلى:

١- أعداد ضخمة من بيانات بطاقات الدفع الاليكترونى، والرقم الشفرى الخاص بكل بنك Algorithm.

٢- مجموعة من الصفحات المصطنعة، والمنسوبة لبعض المؤسسات المالية الأمريكية الكبرى ،استخدمها المتهم كرسائل بريدية خادعة، بهدف الحصول من خلالها على أرقام البطاقات الائتمانية الخاصة بمرتادى الشبكة، وهو الأسلوب الذى يطلق عليه التصيد Phishing،.

٣- عدة آلاف من عناوين البريد الإلكترونى الخاصة بمستخدمى شبكة الانترنت المستهدفين.

٤- برنامج خاص بإعادة تخليق الأرقام الصحيحة لبطاقات الدفع الإلكترونى، المنسوبة للعديد من البنوك الأمريكية.

٥- وبمواجهة المتهمين اعترف كل منهم بنشاطه وقيامه باستلام المبالغ المالية، التى قام بتحويلها لنفسه أو لآخرين، من خلال موقع شركة ويسترن يونيون على شبكة الانترنت.

تحرر عن الواقعة المحضر اللازم، وباشرت النيابة العامة التحقيق وأمرت بحبس المتهمين احتياطياً على ذكة القضية.

هذا وبتطوير مناقشة المتهمين فى تلك الوقائع، اتضح أنهم قد اتخذوا كل وسائل القرصنة والتخفى والخداع، أثناء ممارسة نشاطهم وحتى يصعب التوصل إليهم(*).

---

(*) جميع الجرائم التى تم عرضها للدراسة – السابق ذكرها – من واقع أرشيف الإدارة العامة لمباحث الأموال بوزارة الداخلية، وفى نطاق الاستفادة العملية من العرض دون المزيد من التفصيلات غير المجزئة.

# المبحث الثاني

# الحماية الإجرائية للمعلوماتية في ضوء الاتفاقيات الدولية

## الفرع الأول

## الاهتمام الدولي بالجوانب الإجرائية للجريمة المعلوماتية

### البند الأول: مؤتمر ريو دي جانيرو الدولي الخامس عشر للجمعية الدولية لقانون العقوبات ٤ سبتمبر ١٩٩٤:

أرسى المؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات، والذى عقد فى ريو دى جانيرو بالبرازيل فى الفترة من ٤-٩ سبتمبر سنة ١٩٩٤، جانب هام من المبادئ العامة تتعلق بالقانون الإجرائى، بشأن الجريمة المعلوماتية بيانها(١):

- يتطلب التنقيب L'enquête بالنسبة لجرائم الحاسب الآلى، والجرائم الأكثر تقليدية فى بيئة تكنولوجيا المعلومات - لمصلحة الدفاع الاجتماعى الفعال - أن نضع تحت تصرف سلطات التحقيق Instruction والتحرى Poursuite مكنات قسرية Coercitifs كافية، تتعادل مع الحماية الكافية لحقوق الإنسان وحرمة الحياة الخاصة.
- لتجنب تعسف السلطات الرسمية، فإن القيود التى ترد على حقوق الإنسان عن طريق رجال السلطة العامة، لا يمكن أن تكون مقبولة إلا فى الحالة التى تكون مرتكزة فيها على قواعد قانونية واضحة ودقيقة ومتمشية مع المعايير الدولية لحقوق الإنسان.

---

(1) XV eme congrés international de droit, Rio de Janeiro, Bresil, 409 Septembre 1994, Association internationale de droit penal, R.I.D.P., Ie et 2e trimestres 1995, pp. 32 - 33.

مشار إليه لدى: دكتور/ هلالى عبد اللاه أحمد - تفتيش نظم الحاسب الآلى (دراسة مقارنة)، دار النهضة العربية - سنة ٢٠٠٠ - ص ٥.

الانتهاكات غير المشروعة لحقوق الإنسان التى يرتكبها رجال السلطة العامة، يمكن أن تبطل الدليل المتحصل عليه، بالإضافة إلى تقرير المسئولية الجنائية لرجل السلطة العامة الذى انتهك القانون.

- على ضوء هذه المبادئ العامة يجب أن يحدد بوضوح ما يلى:

أ - السلطات التى تقوم بإجراء التفتيش La perquisition والضبط La saisie فى بيئة تكنولوجيا المعلومات، وخاصة ضبط الأشياء غير المحسوسة Biens non corporels، وتفتيش شبكات الحاسب.

ب- واجبات التعاون الفعال من جانب المجنى عليهم Victimes، والشهود Temoins، وغيروهم من مستخدمى Utilisateurs تكنولوجيا المعلومات، فيما خلا المشتبه فيه Le suspect (خاصة لكى تكون المعلومات متاحة فى صورة يمكن استخدامها للأغراض القضائية fins-judiciaires).

جـ- السماح للسلطات العامة باعتراض Interception الاتصالات داخل نظام الحاسب ذاته، أو بينه وبين نظم الحاسبات الأخرى. مع استخدام الأدلة التى يتم الحصول عليها فى الإجراءات أمام المحاكم.

- نظراً لتعدد وتنوع البيانات المدرجة فى نظم البيانات des systemes de traitement informatique، فإن تنفيذ المكنات القسرية (المنوطة برجال السلطة العامة) يجب أن يكون متناسباً مع الطابع الخطير للانتهاك، ولا يسبب سوى الحد الأدنى من إعاقة gênante الانشطة القانونية للفرد، كما يجب عند بدء التحريات Investigations أن يوضع فى الاعتبار - بالإضافة إلى القيم المالية التقليدية - كل القيم المرتبطة ببيئة تكنولوجيا المعلومات. مثل ضياع فرصة اقتصادية، التجسس، انتهاك حرمة الحياة الخاصة، فقد أو مخاطر الخسارة الاقتصادية، كلفة إعادة بناء تكامل البيانات كما كانت من قبل.

- القواعد القائمة فى مجال قبول ومصداقية الأدلة، يمكن أن تثير مشاكل عند تطبيقها. نظراً لتقييم تسجيلات الحاسبات L'èvaluation des enregistre-

ments informatiques في الإجراءات القضائية، لذا ينبغي إدخال بعض التغييرات التشريعية في حالة الضرورة(*).

كما أوصى مؤتمر ريو دى جانيرور – الدولى الخامس عشر – سالف الذكر – في مجال حركة إصلاح الإجراءات الجنائية وارساء قواعد حماية حقوق الإنسان، بمجموعة من التوصيات بلغت الثلاثين(1)، من أهمها التوصيات التى نعرضها على النحو التالى(**):

---

(*) سبق للحلقة التمهيدية Colloque préparatoire التى عقدت على المستوى الدولى فى فريبورج WURZBOURG بألمانيا بحث «جرائم الحاسب والجرائم الآخرى فى مجال تكنولوجيا المعلومات) فى الفترة من ٥–٨ أكتوبر سنة ١٩٩٢، والتى كانت تمهد لمؤتمر ريو دى جانيرو الدولى الخامس عشر– كما مهدت للمؤتمر السادس للجمعية المصرية للقانون الجنائى الذى أقيم فى القاهرة فى الفترة من ٢٥–٢٨ أكتوبر ١٩٩٣– أن أوصت بما يقارب من التوصيات السابقة الذكر فى مجال التفتيش الإجرائى.

- "Delits informatiques et autres infractions à la Technologie de L'information". Colloque préparatoire, section. I. WURZBOURG, Allemagne 508 Octobre 1992, Associationi.

– وأيضا يراجع: أعمال المؤتمر الدولى السادس للجرائم المعلوماتية المنعقد فى القاهرة – أكاديمية الشرطة – الفترة من ١٣–١٥ أبريل ٢٠٠٥. والذى فى توصياته بتحديث النظام الإجرائى للدول المشاركة – والمنضمة لإتفاقية الجرائم المعلوماتية (أوروبا) – وذلك فيما يتعلق بنصوص تفتيش وضبط نظم الكمبيوتر.

(1) XVem congrès international de droit pénal, op. cit., pp. 36 - 40

(**) التوصية رقم (٢)، يستفيد المتهم من قرينة البراءة La présomption d'innocence فى كل مراحل الإجراءات، حتى صدور حكم يحوز قوة الشئ المقضى فيه.

التوصية رقم (١١): بغض النظر عن التوصية رقم (١٠).. فإن كل إجراء قسرى يتم اتخاذه أو الأمر به من جانب سلطة التحرى أو الشرطة، يجب أن يكون مصدقاً عليه من القاضى فى خلال ٢٤ ساعة.

التوصية رقم (١٤): مجرد اعتراف المتهم لا يقود بالضرورة إلى الإدانة الجنائية، دون فحص صدقه Sa sincérité.

التوصية رقم (١٥): حالات قبول... نتائج المراقبة الإلكترونية عن بعد Des résultats des écoutes électoroniques à distance، يجب أن تكون منظمة بواسطة القانون.

التوصية رقم (١٦): إن منح الإعفاء من العقاب أو تخفيف العقوبة لبعض الشهود Témoins،

=/=

**التوصية رقم (١):**

إن حماية حقوق الإنسان يجب أن تكون مكفولة فى كل مراحل الدعوى الجنائية. بل حتى ولو لم تكن الدعوى قد بدأت بقرار صريح من القاضى أو من موظف عام آخر Un autre fonctionnaire public، ولتحديد لحظة بداية الدعوى، فإن أى إجراء يتخذ من جانب رجال الضبطية القضائية يعتبر كافياً.

**التوصية رقم (٣):**

فى مرحلة التحقيق الابتدائى، والتى تسبق مرحلة المحاكمة، فإن قرنية البراءة تتطلب – إذا ما اتخذت وسائل قسرية -Des moyens coercitifs de prin cipe de proportionnalité – تطبيق مبدأ التناسب الذى يقيم علاقة معقولة بين جسامة الإجراء القسرى فى مساسه بالحقوق الأساسية من ناحية. وبين مدى تناسب هذا الإجراء وفقاً للقصد المتوخى منه من ناحية أخرى.

**التوصية رقم (١٠):**

كل إجراء يتخذ بواسطة سلطة رسمية ويمس الحقوق الأساسية للمتهم – ومنها الإجراءات التى تتخذها الضبطية القضائية – يجب أن يكون مسموحاً به عن طريق القاضى أو خاضعاً لرقابته.

**التوصية رقم (١٢):**

وسائل الإثبات التى تمس بطريقة خطيرة – وخاصة – الحق فى الخصوصية L'intimité، مثل التصنت على المحادثات التليفونية Les ecoutes téléphoniques، لا تكون مقبولة إلا بقرار سابق Préalable من القاضى، وفى الحالات التى قررها المشرع بطريقة واضحة.

= ولبعض المرشدين السريين، لا يكون مقبولاً إلا بصفة استثنائية فى القضايا الخطيرة أو الجريمة المنظمة. وإذا لم يعلن عن هوية هؤلاء الاشخاص فإن إقراراتهم لا تكون لها أى قوة فى الإثبات، ولا يمكن أن تكون أساساً للإجراءات القسرية...

التوصية رقم (١٩): الحق فى الدفاع يكون مكفولاً فى كل مراحل الدعوى.

**التوصية رقم (١٣):**

مجرد البحث عن الأدلة فى المرحلة الابتدائية لا يصلح أن يستخدم كأساس للإدانة.

**التوصية رقم (١٧):**

البحث عن الأدلة، لابد أن يحترم فى كل الفروض السر المهنى Le secret professionnel.

**التوصية رقم (١٨):**

كل الأدلة التى يتم الحصول عليها عن طريق انتهاك حق أساسى للمتهم، والأدلة المستمدة منها تكون باطلة، ولا يمكن مراعاتها فى أى لحظة خلال الإجراءات.

**التوصية رقم (٢٠):**

لا يجبر أحد على أن يساعد بأسلوب إيجابى – مباشرة أو بطريقة غير مباشرة – فى اتهام نفسه جنائياً.

المتهم له الحق فى الصمت Se tair .. وصمته لا يستخدم ضده Son silence ne sera utilisé contre lui.

**البند الثاني: أتفاقية بودابست ٢٠٠١ بشأن الاجرام المعلوماتي:**

فى عام ١٩٨٩ نشر المجلس الأوروبى(*) دراسة تضمنت توصيات بضرورة

---

(*) المجلس الأوروبى The council of Europe يتكون من ٤١ دولة، وقد تأسس عام 1949 كاتحاد Forum مضاد للأفكار الدكتاتورية التى سادت أوروبا فى النصف الأول من القرن العشرين، ولتقوية حركة الدفاع عن حقوق الانسان، وتطوير الحركة الديمقراطية ودور القانون فى هذا الأطار، وعلى مدى سنوات عد المجلس الأوروبى الملجأ الأمين للدول الأوروبية لكل حوار يمكن أن يكون مفيداً وتنبثق عنه اتفاقيات فى هذا الاطار بين الدول الأعضاء فيه. (د/ عمر محمد بن يونس – الاتفاقية الأوروبية للجريمة الافتراضية –مرجع سابق – ص ١٣).

تفعيل دور القانون لمواجهة الأفعال غير المشروعة عبر الحاسوب، ومن ذلك التوصية رقم 9 (S9) Recommendation No. R.، وهى التوصية التى لحقتها دراسة أخرى فى عام ١٩٩٥ حول الإجراءات الجنائية فى مجال جرائم الانترنت والتى تضمنتها التوصية 13 (95) Recommendation No. R.. وعلى أساس المبادئ التى تضمنتها هاتان التوصيتان قام مجلس أوروبا فى عام ١٩٩٧ بتشكيل لجنة خبراء الجريمة عبر العالم الافتراضى Committee of Experts on crime in cyberspace (PC-CY) وذلك بقصد إعداد اتفاقية فى هذا الإطار، تتضمن فى محتواها ضرورة تسهيل التعاون الدولى فى الإجراءات، فى الجرائم الناشئة عن استخدام الحاسوب والانترنت(١).

وفى أبريل عام 2000 صدر أول مشروع Draft لهذه الاتفاقية بعنوان:

«اتفاقية الجريمة عبر العالم الافتراضى / الإنترنت The cybercrime convention» لكى تكون معيناً للدول فى مواجهة الجريمة فى العالم الافتراضى/الانترنت، حيث وافقت عليه ثلاثة وأربعون دولة أوروبية الأعضاء فى المجلس الأوروبى. ولقد كان المشروع الأول من هذه الاتفاقية (مشروع ابريل2000) ناقصاً، فلم يتضمن العديد من الجرائم التى تعد فى نظر المتخصصين فى قانون الإنترنت من الجرائم التى يلزم أن يتضمنها القانون المقارن والدولى فى نصوص جنائية، كما هو الشأن فى جرائم الاختراق وغيرها(*).

---

(1) DRAFT Convetion on Cyber-Crime And Explanatory Memorandum Related The Reto (final Activity Report). Secretariat Memorandum Prepared by the Directorate General of Legal Affairs, Strassbourg, 25 May 2001, CDPC (2001) 2 rev.

(*) هى جرائم تقنية متعلقة تخصيصاً بالانترنت ومن طبيعتها، بحيث يلزم هيكلتها فى كل دراسة تعد لذلك وهو الأمر الذى اتخذ منه القضاء المقارن (سيما الأمريكى والإنجليزى) ذريعة لحث المشرع على إصدار تشريعات تعاقب على أشكال الاختراق جنائياً.

ولعله من الجديد بالذكر أن الاتفاقية تضمنت ما يفيد اهتمام المجتمع الدولى بموضوع الجريمة عبر الأنترنت، فهى تعبير حقيقى عن الأهتمام الدولى بهذه النوعية من الجرائم. فالاتفاقية

-/-

وفى أكتوبر/ نوفمبر 2000(*) – أصدر الاتحاد الأوروبى المشروع المعدل لهذه الاتفاقية، ويتكون من (48) مادة تتضمن – فضلاً عن نصوص تجريم وعقاب – جانباً من محاولة الاتحاد الأوروبى حصر مجالات التعاون الدولى فى إطار الإجراءات الجنائية.

ومن حيث الإجراءات فقد أوصت الاتفاقية (بودابست ٢٠٠١) الدول الأعضاء بالتالى:

– اتخاذ الإجراءات الضرورية لمراقبة نظم المعلومات فى المنظمات التى يلاحظ تعاملاتها الإجرامية. واستناداً إلى هذه التوصية أصدر المشرع الفرنسى القانون المؤرخ فى 2000/8/1 بتعديل القانون المؤرخ 1986/9/30 بشأن حرية الاتصالات، حيث تضمن مسئولية مزود الدخول والخدمات عبر الإنترنت(**).

---

وضعت أساساً أولياً لامكانية التعاون الدولى فى مجال المكافحة الدولية للجريمة عبر الإنترنت، حيث أنها أبرزت هذا الاتجاه – لأول مرة – لكى يتحول النداء إلى واقع ملموس فى هذا الشأن فقد تضمنت الاتفاقية فى موضوعها ثلاثة أقسام كبير:

- **يتناول القسم الأول:** مجموعة الجرائم التى يمكن أن يتعرض لها الحاسب الآلى والأنترنت، ويشار هنا إلى أن مجموعة الجرائم انما هى **نقل موسع** عن الجرائم المقررة فى التشريع الأمريكى أساساً.
- **ويتناول القسم الثانى من الاتفاقية:** مجموعة الإجراءات الجنائية التى يمكن أن تتخذ فى مواجهة هذه النوعية من الجرائم.
- **وتضمن القسم الثالث:** موضع التعاون الدولى بين الدول الأعضاء الموقعين على الاتفاقية.

(*) تم توجيه الدعوة إلى الولايات المتحدة الأمريكية واليابان وجنوب أفريقيا وكندا لكى تشارك كل منها فى اعداد هذه الاتفاقية بصفة مراقب Observer، وذلك منذ توصية 1989 مروراً بتوصية 1995، وأيضاً فى إطار اعداد الاتفاقية ذاتها لكون الولايات المتحدة الأمريكية تحديداً ذات علاقة مصلحة مباشرة بموضوع الجريمة عبر الانترنت. أما مشاركة كل من كند واليابان وجنوب افريقيا فى اعداد الاتفاقية فهو الأمر الذى يجعل الاتفاقية صالحة لكل تمتد إلى غير الأعضاء فى الاتحاد الأوروبى، من حيث إمكانية الدول غير الأعضاء فى الاتحاد للدخول فيها. ومن ثم سمح المشروع للدول غير الأعضاء فى الاتحاد الأوروبى التقدم بطلب عضوية (م ٤٨ من المشروع المعدل الصادر فى نوفمبر 2000). (د/ عمر محمد بن يونس – المرجع السابق – ص ١٤).

(**) إذا سمح المشرع الفرنسى بمقتضى هذا القانون لمزودى الخدمات بمراقبة حركة أعضاء الانترنت.

- تفتيش وضبط البيانات المخزنة ذات القيمة المعلوماتية.

ويلزم هذه التوصية ضرورة استحداث مواءمة بين الوثائق المادية Docu-ments وبين البيانات المعلوماتية Donneés informaiques، وكذلك تنظيم إجراءات الضبط La saisie نسخ البيانات المعلوماتية، وإمكانية حصول سلطات التحقيق على نسخ من البيانات المذكورة، حيث ورد فى مشروع القانون الفرنسى بشأن مجتمع المعلوماتية Loi sur la société de l'information ما تضمن لزوم تعديل الموارد (97-56) من قانون الإجراءات الجنائية الفرنسى للوصول إلى المواءمة المذكورة.

- تجميع البيانات في الزمن الفعلي / المادي En temps Reel كتدبير وقائي.

حيث سمحت الاتفاقية للدول الأعضاء بإعداد نظم مراقبة الاتصال بالإنترنت، عبر منظومة الاتصالات التقليدية للتعرف على كنة السلوك الإتصالى بالإنترنت، وفيما إذا كان سلوكاً خطراً من عدمه(*).

وفى 2001/5/25 صدر التقرير النهائى لمشروع الاتفاقية عن اللجنة الأوروبية لمشكلات الجريمة(**)، ممثلة فى لجنتها الفرعية – لجنة خبراء

---

(*) كانت أبرز النقاط التى أثيرت حول الاتفاقية، وجعلت التشكيك فيها يصل إلى مرتبة العدوان على الحق فى الخصوصية والعدوان على الحق فى التعبير، هى مسألة توضيح مدى امكانية منح مزود خدمات الانترنت ISP الحق فى الاحتفاظ بالبيانات المطلوبة Data retention requirement. على أن اتجاها فى إطار هذه الاتفاقية رفض الاعتراف بأن لمزود الخدمات مثل هذه الصلاحية، وكل ما هناك أن لمزود خدمات الانترنت دور حال اتخاذ اجراءات جنائية ضد مرتكب جريمة ما، بحيث يكون عمله مقيداً فى اطار التحفظ على الأدلة Preservation requirement فيبدو دوره محصوراً فى تمكين سلطات التحقيق من علمهم حال وجود جريمة تتخذ بشأنها اجراءات جنائية من تتبع وتعقب مرتكبها فى أى مكان. والتحفظ Preservation على الأدلة ليس بالفكرة الجديدة. (د/ عمر محمد بن يونس – المرجع نفسه –ص ص ٢١، ٢٢).

(**) (CDPC) European Committee on Crime Problems -

وقد تضمن التقرير النهائى السعى إلى تحقيق عدة أهداف هى:

– إحداث تناسق فى عناصر الحكم الموضوعى للجرائم عبر العالم الافتراضى.

-/-

الجريمة فى العالم الافتراضى(*). وتبع ذلك فى 2001/11/23 فى بودابست / المجر تم التوقيع على الاتفاقية(**). ومن أهم الملاحظات على الاتفاقية – بعد دخولها حيز التصديق – ما يتعلق بفكرة البناء الهيكلى للجريمة عبر الأنترنت.

- فمن حيث الركن المادي للجريمة في العالم الافتراضي:

اعترفت الاتفاقية بكونها ذات طابع توجيهى ملزم، فالمادة الثانية من الاتفاقية تقرر إنه: «يلتزم كل عضو – فى هذه الاتفاقية – بإصدار تشريع واتخاذ الإجراءات الأخرى الضرورية لتقنين الجريمة Criminal offences وفقاً لما هو مقرر فى نظامها القانونى Domestic law، حال ارتكابها بشكل عمدى».

---

– العمل على توفير الفاعلية للإجراء الجنائى الضرورى للتحقيق والاتهام فى الجرائم المرتكبة باستخدام الحاسوب والانترنت بقصد الحصول على الدليل فى هيئته الإلكترونية/الرقمية.

– إعداد نظام سريع وفعال للتعاون الدولى فى مجال الجريمة عبر الانترنت.

– عدم ربط مزود الانترنت Provider بالنظام الأمنى للدولة.

(*) - (PC - Cy) Committee of Txperts on crimein cyber-Space

وتضمن هيكلة المشروع للاتفاقية ثلاثة اتجاهات كبرى كسياسة عامة للاتفاقية، وهذه الاتجاهات تتمثل فى:

أولاً: لزوم أن تكون الاتفاقية مرتكزاً تلتقى عنده حركة التشريع فى كل دولة عضو فى الاتحاد (بالإضافة للدول الأربعة المشاركة)، وفقاً للمادة (1/36) من الاتفاقية، مع مراعاة ما تقرره المادة (48) التى سمحت لغير الدول المشار إليها فى الانضمام إلى الاتفاقية، طالما قبلت بما تتضمنه من شروط تتعلق بها، حيث قامت الاتفاقية بتحديد ملتقى مركزى لأنواع الجرائم التى يجب أن تكون متضمنه فى التشريعات الوطنية للدول الأعضاء. وهى على التوالى: الجرائم المتعلقة بأمن الشبكات، والجرائم المعلوماتية، وجرائم الاخلاق، وجرائم العدوان على حقوق الملكية الأدبية والفكرية، وجرائم ضد الجنس البشرى.

ثانياً: الأهتمام بالإجراءات الجنائية. سيما فى مرحلة التحقيق والملاحقة القضائية عبر العالم الافتراضى.

ثالثاً: تحوير الاتفاقية لكى تحظى باهتمام وسائل التعاون الدولى، بقصد تحقيق أفضل النتائج فى مكافحة الجريمة عبر العالم الافتراضى.

(**) قامت ثلاثون دولة أوروبية بالتوقيع على الاتفاقية، بما فى ذلك ا لدول الأربعة من غير الأعضاء فى المجلس الأوروبى، المشاركة فى إعداد هذه الاتفاقية (وفقاً للمادة 36 من الاتفاقية)، وهى كندا واليابان وجنوب أفريقيا والولايات المتحدة الأمريكية.

إلا أن الالتزام المشار إليه ليس له سوى أثر رجعى، حيث ان الدول الأعضاء فى اعداد هذه الاتفاقية تملك تشريعات من هذا النوع.

على أن الجديد فى هذا الأطار هو اعتراف الاتفاقية المذكورة بكون النشاط التقنى يعد جزءاً لا يتجزء من النشاط المادى في مثل هذه النوعية من الجرائم. ومثل هذا الأمر يعد تطويراً فى فهم آلية الجدل التى تكتنف الجرائم الناشئة عن استخدام الانترنت(١). ويبرز هذا التأكيد بشكل واضح فى المادة الثالثة من الاتفاقية التى تضمنت مصطلحاً باستخدام التقنية By Technical Means.

- وفيما يتعلق بالركن المعنوي:

فالملاحظ اعتراف الاتفاقية الأوروبية بصورة واحدة فقط للقصد الجنائى لبناء(*) المسئولية الجنائية Criminal liability، وهذه الصورة هى العمد بترديدها لمصطلح Interntionally. ويعنى هذا المصطلح تحديد الإرادة فى معنى «يريد أن يترتب على عمله». حيث يستخدم مشرع الاتفاقية عبارة "When Commit-ted Intentionalty".

وبعد فإن عرض ما سلف من تمهيد للجوانب الإجرائية التى تتناول الجريمة المعلوماتية،، أنما مقصده عرض لرؤية تناولها المشرع الأوروبى بجراءة، وهو يرسى اتفاقاً دولياً بين مجموعة من الدول، تتمثل هذه الرؤية فى توحيد المصطلحات المتناولة للإجرام التقنى الافتراضى الذى يتناول الجرائم المعلوماتية. وما يقوم به المشرع الأوروبى هو مجاراة تنسيقية لما هو مقرر فى لجان اعداد نماذج التشريعات، وهى لجان ينضم إليها متخصصون بشكل مستمر

---

(١) د/ عمر محمد بن يونس – المرجع السابق – ص ٣١.

(*) أخذت الاتفاقية بتقسيم فكرة القصد الجنائى إلى قصد عام وآخر خاص Specific intentional element فى بعض الجرائم. وذلك مثلما هو مقرر فى المادة (8) من الاتفاقية التى تتعلق بالنصب Fraud عبر الانترنت، حيث تطلب مشرع الاتفاقية صورة خاصة وهى تحقيق مكسب اقتصادى Economic benelit – ولقد صدر للاتفاقية ملحق فى بروتوكول أضافى فى 2003/1/28 يتضمن تجريم العنصرية والرهبة من الأجانب Racist and xenophobic material.

تسعى إلى رصد الظواهر الاجرامية الحديثة وصياغة سياج قانونى يسمح بالتعامل معها بل ومواجهتها. ولعل ذلك يكون مصدر من مصادر عديديه لا تنضب، يمكن للمشرع الوطنى والمشرع العربى أن يستفيد منه ويحزو حزوه أن أمكن له تنفيذ ذلك، فمن غير المعقول – ولم يعد مقبولاً – أن تواجه جرائم القرن الحادى والعشرين بنصوص قانونية ونظم إجرائية وضعت فى بدايات القرن الماضى.

## الفرع الثاني

## المشكلات العملية بشأن الحماية الإجرائية للمعلوماتية في ضوء اتفاقية بودابست

أدت الثورة التكنولوجية La révolution technologique[1] التى تشتمل على الطريق السريع الإليكترونى L'inforoute[2] بنماذجه المختلفة للاتصال والخدمات والتى تترابط وتتشابك عبر طرق البث ونقل المعلومات، إلى تشوش Bouleversé دائرة قانون العقوبات وقانون الإجراءات الجنائية. فالنمو الدائم لشبكات الاتصال يفتح آفاقا جديدة للإجرام Ouvre de nouvelles perspectives à la criminalité[3] سواء فيما يتعلق بالجرائم التقليدية Des infractions classiques[4] أو الاجرام التكنولوجى الجديد La nouvelle criminalité technologique[5] وفى هذا الصدد لا يكفى أن يكون قانون العقوبات فقط متماشياً مع هذه الجرائم الجديدة، بل يجب أن يشمل هذا التطور أيضاً قوانين الإجراءات الجنائية وتقنيات التنقيب والتحرى Des techniques d'enquêté وبنفس الطريقة، يجب

---

(١) ويقابل ذلك فى ا لمصطلح الإنجليزى The technological revolution.

(٢) ويقابل ذلك فى المصطلح الإنجليزى "The "electronic highway.

(٣) ويقابل ذلك فى الطبعة الإنجليزية Opens new doors for criminal activity.

(٤) ويقابل ذلك فى المصطلح الإنجليزى Traditional offences.

(٥) ويقابل ذلك فى المصطلح الإنجليزى New techological crimes.

اتخاذ احتياطات Des sauvegardes[1] تسمح بأن يكون لها تأثير على البيئة التكولوجية الجديدة، وعلى تطوير سلطات الإجراءات الجديدة.

**البند الأول: بيان مشكلات الحماية الإجرائية للمعلوماتية:**

أحدى المشاكل الأكثر صعوبة التى تطرح للكفاح ضد الإجرام فى عالم الشبكات L'univers des réseaux[2] هو صعوبة تحديد فاعل الجريمة La difficulté d'identifier L'auteur d'une infraction وتقييم مدى وأثر الجريمة Evaluer la portée et l'impact de celle. ci.[3]

وهناك مشكلة أخرى تتعلق بتبخر البيانات La volatilité Des données électroniques التى يمكن أن يتم تعديلها Modifiées، أو تغييرها Deplacées أو محوها Effacées فى بضع ثوان En quelques secondes وهكذا، على سبيل المثال، فإن المستخدم Utilisateur الذى يتحكم فى البيانات Qui contrôle les données[4] يمكن أن يستعمل نظاماً معلوماتياً من أجل محو تلك البيانات التى تعد موضوعاً للتنقيب الجنائى Qui font l'objet d'une enquête pénale[5] وبالتالى يدمر كل الأدلة[6] Détruisant ainsi toutes les preuves ولذلك فإن السرعة La rapidité، وأحياناً السرية Le secret تعدان فى غالب الأحيان من العناصر الجوهرية فى نجاح التنقيب والتحرى Des ingrédients

---

(١) ويقابل ذلك فى المصطلح الإنجليزى Investigative techniques.

(٢) ويقابل ذلك فى الطبعة الإنجليزى The difficulty in identifying the perpetrator.

(٣) ويقابل ذلك فى الطبعة الإنجليزية Assessing the extent and impact of the criminal Act.

راجع فى ذلك: د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والاجرائية لجرائم المعلوماتية – مرجع سابق – ص ١٦٠ وما بعدها.

(٤) ويقابل ذلك فى الطبعة الإنجليزية Who is in control of the data.

(٥) ويقابل ذلك فى الطبعة الإنجليزية That is the subject of a criminal investigation.

(٦) ويقابل ذلك فى الطبعة الإنجليزية Destroying the evidence.

essentiels du succés d'une enquête وتتبنى الاتفاقية وسائل إجرائية تقليدية Les procédures classiques مثل التفتيش La Pérquistion والضبط La Saisie في الوسط التكنولوجي الجديد. Au nouveau milieu technologique وعلى التوازي تتبنى أيضاً إجراءات جديدة، مثال ذلك التحفظ العاجل على البيانات La conservation rapide de données[1] بطريقة تضمن أن الإجراءات التقليدية لجمع البيانات كالتفتيش والضبط لا تزال فعالة Demeurent effectives في بيئة تكنولوجية تتميز بالتلاشي أو التبخر Caractérisé par la volatilité.

ونظراً لأن البيانات ليست دائماً ساكنة Statiques لكنها متدفقة عبر إطار عملية الاتصال Circulant dans le cadre du processus de communication[2] فإن الإجراءات التقليدية الأخرى لجمع الأدلة والمتعلقة بالاتصالات، مثال ذلك الجمع في الوقت الفعلي La collecte en temps réel البيانات المرور Données de trafic[3] والاعتراض في الوقت الفعلي لبيانات المحتوى L'interception en temps réel des donneés de contenu[4] قد تم تبنيها أيضاً من أجل إمكان جمع الأدلة الإليكترونية أثناء عملية الاتصال ذاتها. بعض هذه الإجراءات مشار إليها في توصية رقم ١٣ (٩٥) La Recommandation No. (95) 13 لمجلس أوروبا الخاصة بمشاكل الإجراءات الجنائية المرتبطة بتكنولوجيا المعلومات.

كل البنود المشار إليها في هذا القسم تهدف إلى السماح بالحصول أو جمع البيانات بهدف التنقيبات أو الإجراءات الجنائية التي تقود إليها. واتصالاً بهذا قام واضعوا الاتفاقية الحالية بمناقشة مسألة ما إذا كان يجب أن تفرض الاتفاقية على مقدمي الخدمات Fournisseurs de services الالتزام بالتجميع والاحتفاظ منهجياً ببيانات المرور خلال دورة محددة من الزمن، لكن لم يتم إدراج مثل هذا الالتزام بسبب عدم الموافقة الجماعية عليه.

---

(١) ويقابل ذلك في الطبعة الإنجليزية Expedited preservation of data.

(٢) ويقابل ذلك في الطبعة الإنجليزية Flowing in the process of Communication.

(٣) ويقابل ذلك في الطبعة الإنجليزية Real - Time collection.

(٤) ويقابل ذلك في الطبعة الإنجليزية Interception of content data.

وبطريقة عامة، فإن الإجراءات المرتبطة بكل نماذج البيانات بما فى ذلك ثلاثة أنواع خاصة بالبيانات المعلوماتية (البيانات المتصلة بالمرور، وبيانات المحتوى، وبيانات المشترك Les données relatives aux abonnés يمكن أن تتبلور فى شكلين: مخزنة أو مسجلة Enregistrées أو فى طورا لانتقال En cours de transmission[١] كما سنجد أن تعريف بعض هذه المصطلحات قد ورد فى المادتين ١ و ١٨. كذلك فإن إمكانية تطبيق إجراء معين على نوع أو شكل معين من البيانات المعلوماتية، يعتمد على طبيعة وشكل البيانات، وطبيعة الإجراء الذى يشكل موضوع الوصف الخاص لكل مادة[٢].

وفيما يتعلق بتوافق الإجراءات التقليدية مع البيئة التكنولوجية الجديدة Le nouvel environnement techologique[٣] فإن مسألة المصطلحات المناسبة تطرح نفسها فى كل نصوص هذا القسم الحالى. والخيار Le choix يكون بين الاحتفاظ بالمصطلح التقليدى، مثال. فتشPerquisitonner وضبط Saisir أو استخدام مصطلحات معلوماتية جديدة وأكثر قرباً من الوسط التكنولوجى، مثال ولج Accéder ونسخ Copiere تلك المصطلحات التى تم تبنيها فى نصوص المواثيق الدولية المهتمة بهذا الموضوع. كما هو الحال بالنسبة للمجموعة الفرعية لدول لثمانى حول إجرام التكنولوجيا المتقدمة Le sous Groupe sur La crimi-nalité de haute technologie du G G8[٤]. والخيار الثالث هو اتخاذ حل وسط Une solution de compromis[٥] مثال: فتش Perquisitionner أو ولج Accéde بأى طريقة مشابهة، وضبط Saisir أو حصل Obtenir بأى طريقة مشابهة.

---

(١) ويقابل ذلك فى الطبعة الإنجليزية In the Process of Communication.

(٢) راجع د/ عمر محمد بن يونس – الترجمة العربية لاتفاقية بودابست ٢٠٠١ – مرجع سابق – ص ١٤ بشأن المادة (١٨) أمر استخراج الدليل Production order.

(٣) ويقابل ذلك فى الطبعة الأنجليزية The new technological environment.

(٤) ويقابل ذلك فى الطبعة الإنجليزية The G 8 High tech crime subgroup.

(٥) ويقابل ذلك فى الطبعة الإنجليزية Employing a compromise of mixed language.

كمـا أنه من الأهميـة الأخـذ فى الحـسبـان تطور المفـاهيم فى الوسط الإليكترونى L'évolution des concepts dans le milieu électronique مـع تحـديدها والاحـتفـاظ بجذورها التـقليـدية Leurs racines traditionnelles[(١)].

وبالتالى فـهناك حاجـة ماسة إلى الأخـذ بمدخل مرن L'approche souple يسمح للدول باسـتـخدام امـا المقـولات التـقليـدية Les notions classiques كالتفتيش والضبط، وأما المقولات الجديدة Les notions nouvelles كالولوج والنسخ.

وأخيراً، فإن كل مواد هذا القسم تشير إلى مصطلح «السلطات المختصة Les autorités compétentes»، والسلطات Les pouvoirs التى يجب أن تمنح بغرض التنقيبات Des enquêtes أو الإجـراءات الجنائيـة فى بعض البـلاد، فـإن القضـاة وحدهم Seuls les Juges هم الذين يناط بهم سلطة الأمـر أو التـصريح بـجمع أو إنتاج عناصر الإثبات Le pouvoir d'ordonner ou d'autoriser la collecte ou production d'éléments de preuve بينما فى بلدان أخـرى يقوم ممثلو الإدعـاء Les procureurs[(٢)] أو ممثلو تطبيق القانون الآخـرون بهـذه المهمـة. ولذلك يتم تسليحهم بنفس السلطات أو بسلطات مشابهة.

وعلى ذلك فإن مصطلح «السلطة المختصـة Autorité compétente» يعنى سلطة قضائية، أو إدارية، أو بوليسية مؤهلة قانوناً Policiére habilité فى القانون الداخلى يناط بها الأمـر، أو التصريح، أو مبـاشرة تنفيذ إجراءات جمع أو إنتـاج عناصر الإثبات، المرتبطة بالتنقيبات والإجراءات الجنائية[(٣)].

---

(١) ويقابل ذلك فى الطبعة الإنجليزية The old notions بمعنى المقولات القديمة وهى تسمية غير دقيـقة. وذلك لأن هناك فارقاً بين التـقليدى والقديم، فكلمـة قديم تطلق على الشئ الذى كان يستخدم فى الماضى ولم يعد يستخدم الأن، أما التقليدى فيطلق على الشئ الذى كان يستخدم فى الماضى ومازال استخدامه شائعاً فى الحاضر.

(٢) ويقابل ذلك فى المصطلح الإنجليزى Procecutors.

(٣) د/ هلالى عبد اللاه أحمد - المرجع السابق - ص ١٦٤.

**البند الثاني: من إجراءات حماية نظم المعلوماتية:**

فى اطار إرساء قواعد إجرائية (وطنية) تهدف إلى حماية النظم المعلوماتية. يمكن الاسترشاد بالاتفاقيات الدولية المبرمة بشأن المعلوماتية(١)، حيث تضمنت اتفاقية بودابست 2001 إجراء التحفظ العاجل على البيانات المعلوماتية المخزنة Conservation rapide de données d'informatiques stockées وتشير المذكرة التفسيرية للإتفاقية إلى أن الإجراءات الواردة فى المادتين 16 ، 17(*)، تنطبق على البيانات المخزنة au données stockées التى سبق تجميعها Collectées والاحتفاظ بها Archivées عن طريق حائزى البيانات Les détenteurs de don-nées، مثال ذلك مقدمى الخدمات.

---

(١) د/ هلالى عبد اللاه أحمد – الجوانب الموضوعية والاجرائية لجرائم المعلوماتية – مرجع سابق – ص ١٨٦ وما بعدها، ود/ عمر محمد بن يونس – الترجمة العربية للمذكرة التفسيرية للاتفاقية الأوروبية للجريمة الافتراضية – مرجع سابق – ص ١٣٠ وما بعدها.

(*) المادة (16) التحفظ العاجل على البيانات المعلوماتية المخزنة:

١- يجب على كل طرف أن يتخذ الإجراءات التشريعية، وأية إجراءات أخرى يرى أنها ضرورية من أجل السماح لسلطاته المختصة أن تأمر أو أن تفرض بطريقة أخرى التحفظ العاجل على البيانات المعلوماتية المخزنة، وبما فى ذلك البيانات المتعلقة بالمرور المخزنة بواسطة نظام معلوماتى، وبالأخص عندما تكون هناك أسباب تدعو للاعتقاد بأن هذه البيانات على وجه الخصوص معرضة للفقد أو التغيير.

٢- عندما يقوم طرف بتطبيق الفقرة «١»، أعلاه، عن طريق أمر يصدر لشخص للتحفظ على البيانات المخزنة الموجودة فى حوزته أو تحت إشرافه، فإن هذا الطرف يجب عليه اتخاذ الإجراءات التشريعية والإجراءات الأخرى التى يراها ضرورية من أجل إجبار هذا الشخص على التحفظ وحماية سلامة البيانات المذكورة لمدة طويلة من الزمن على قدر الضرورة، بحد أقصى ٩٠ يوماً بغرض السماح للسلطات المختصة بالكشف عنها. كما يمكن لكل طرف أن يقرر تجديد هذا الأمر.

٣- يجب على كل طرف اتخاذ الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية لإجبار حارس البيانات، أو أى شخص يقع عليه عبء التحفظ على هذه البيانات، أن يحافظ على السرية بالنسبة لتطبيق الإجراءات المذكورة خلال المدة المقررة بواسطة قانونه الداخلى.

المادة (17) التحفظ والإفشاء العاجلان لبيانات المرور:

-Conservation et divulgation raides de données relatives au tralic.

-/-

والإجـراءات المقـررةفى هاتين المادتين لا تطبق إلا إذا كـانت البـيـانات المعلومـاتيـة أو بيـانات الحـاسب موجـودة من قـبل وفى طور التـخـزين Existent déjà et sont en cours de stockage لكن لأسباب عـديدة قد لا تكون البيـانات المعلومـاتيـة أو بيانات الحـاسب فى تعـبيـر آخـر، التى تمثل مـصلحـة للتـنقـيـبات الجنائيـة موجـودة N'existent pas، أو لم تعـد مـخـزنة Ne sont plus stockées فعلى سبيل المثال، قد لا يتم تجميع بيانات دقيقة، ولا الاحتفاظ بها، أو قد يتم تجميعها، ولكن لا يتم الاحتفاظ بها. كما أن القوانين المنظمة لحماية البيانات يمكن أن تفرض تدمير بيانات هامة Destruction de données importantes قبل أن تتحقق من أهميتها بالنسبة للإجراءات الجنائية، كذلك فى بعض الأحيان قـد لا يكون هـناك باعـث تجـارى Motif commercial من أجل تجـمـيـع أو الاحتفاظ بالبيانات، كما هو الحال عندما يدفع العملاء Les clients مبلغاً جزافياً Un tarif forfaitaire نظيـر الخـدمـات، أو أن تكون الخـدمـات مـجـانيـة. كل هذه الأمور لا تعالجها المادتان ١٦ ، ١٧.

وإنه من الأهمية بمكان إقامة تفرقة بين مصطلحى: «التحفظ على البيانات La conservation des données»[(١)] و «الاحتفاظ أو أرشفة البيانات l'archivage des données»[(٢)] فرغم أن للكلمتين معنيين متجاورين Des sens voisins فـى

---

١- من أجل ضمان التحفظ على البيانات المتعلقة بالمرور فى تطبيق المادة (16)، يجب على كل طرف اتخاذ الإجراءات التشريعية وأية إجراءات أخرى يرى أنها ضرورية من أجل: -
أ - التأكد من أن التحفظ العاجل لهذه البيانات المتعلقة بالمرور متوافر، بغض النظر عما اذا كان هناك مقدم خدمة واحد أو عدة مقدمين للخدمة قد ساهموا فى نقل الاتصال.
ب- ضمان الإفشاء السريع، للسلطة المختصة للطرف أو للشخص المعين من قبل هذه السلطة، عن كمية بيانات مرور كافية، تسمح بتحديد هوية مقدمى الخدمات والطريق الذى تم الاتصال من خلاله.

(١) ويقابل ذلك فى المصطلح الإنجليزى "Data Preser vation".

(٢) ويقابل ذلك فى المصطلح الإنجليزى "Data retention".

اللغة الشائعة لكن لهما معنى مختلف فى لغة المعلوماتية. إذ إن عبارة «يتحفظ على البيانات Conserver des données»[1] تعنى حفظ بيانات سبق وجودها فى شكل مخزن Stockée وحمايتها من كل شئ يمكن أن يؤدى إلى إتلافها Alterer أو تجريدها من صفتها Dégrader la qualité أو حالتها الراهنة L'état actuel.

فى حين أن عبارة: «الاحتفاظ بالبيانات L'archivage des données»[2] تعنى حفظ البيانات لدى حائزها بالنسبة لمستقبل البيانات التى فى طور الإنتاج أو التوالد. فأرشفة البيانات يشير إلى تجميع البيانات فى الوقت الحاضر وحفظها أو حيازتها – فى أرشيف أى وضعها فى ترتيب معين والاحتفاظ بها فى المستقبل. ومعنى ذلك أن «أرشفة البيانات L'archivage des données» عبارة عن عملية تخزين للبيانات Le données processus de stockage des[3] على عكس «التحفظ على البيانات La conservation des données» الذى يعنى النشاط الذى يضمن للبيانات سلامتها وسريتها Garantit leur Sécurité et leur sûreté L'activité qui[4].

وعلى ضوء تلك التفرقة السابقة، فإن نطاق المادتين ١٦، ١٧ يقتصر على «التحفظ على البيانات La conservation des données» ولا يمتد إلى «الاحتفاظ بها Non leur archivage». كما أن المادتين لا يتضمنان ما يوجب الجمع La collecte والاحتفاظ L'archivage بكل أو حتى بعض البيانات المجمعة بواسطة مقدم خدمات un fournisseur de services أو أى كيان آخر Une autre entilé فى إطار أنشطته. وإجراءات التحفظ على البيانات Les mesures de conservation تنطبق على بيانات معلوماتية Aux données électroniques أو بيانات الحاسب التى «تم تخزينها Stockées عن طريق نظام معلوماتى» Stockées au moyen d'un sys-

(١) ويقابل ذلك فى المصطلح الإنجليزى To preserve data.

(٢) ويقابل ذلك فى المصطلح الإنجليزى Data retention أو To retain data.

(٣) ويقابل ذلك فى الطبعة الإنجليزى Is the process of storing data.

(٤) ويقابل ذلك فى الطبعة الإنجليزية Is the activity that keeps that stored data secure and safe

teme informatique. وهو ما يفترض أن البيانات موجودة من قبل وتم تجميعها وتخزينها.

وعلاوة على ذلك، كما يشار إلى ذلك فى المادة ١٤(*)، فإن كل السلطات والإجراءات المطلوب تأسيسها أو إنشائها فى القسم الثانى من Les pouvoirs الاتفاقية يجب أن تكون «بهدف التنقيبات أو الإجراءات الجنائية النوعية Aux fins d'enquêtes ou de procédures pénales spécifiques. وهو ما يقيد تطبيق الإجراءات على تحقيق معين فى قضية معينة. بالإضافة إلى ذلك، عندما يقوم طرف بتطبيق إجراءات التحفظ عن طريق إصدار أمر Au moyen d'une or-donnance فإن هذا الأمر يكون مقتصراً على: «بيانات مخزّنة نوعية لدى شخص أو تحت سيطرته Des données stockées spécifiées se trouvant en la possession ou sous le contrôle de la personne» (الفقرة ٢ من المادة ١٦) وعلى ذلك فإن المادتين ١٦، ١٧ تقرران فقط سلطة طلب التحفظ على بيانات متواجدة ومخزنة فى انتظار الكشف عن محتواها، لسلطات قانونية أخرى، بمناسبة التنقيبات والتحقيقات الجنائية النوعية.

الالتزام بضمان التحفظ على البيانات L'obligation d'assurer لا يقصد منه الزام الأطراف بقصر تقديم أو استخدام خدمات لا يستعملونها بشكل منتظم أو روتينى فى التجميع Collecter أو الاحتفاظ Archiver ببعض نماذج من البيانات، مثال ذلك بيانات المرور أو المشتركين Aux abonnés فى إطار الممارسات التجارية المشروعة.

---

(*) المادة (١٤) نطاق تطبيق نصوص قانون الإجراءات الجنائيةChamps d'application des mesures du droit de procédure.

فقرة (١): يجب على كل طرف أن يتخذ الإجراءات التشرعية، وأية إجراءات أخرى يرى أنها ضرورية من أجل إنشاء السلطات والإجراءات المنصوص عليها فى هذا القسم بغرض التنقيبات أو الإجراءات الجنائية الخاصة.

كما أنه لا إلزام على الأطراف بتطبيق إمكانيات تكنولوجية جديدة من أجل هذا الغرض. أى الاحتفاظ ببيانات، يمكن أن توجد على الجهاز لمدة معينة من أجل الإجابة عن طلب Une demande أو أمر Une injonction.

ومع ذلك هناك بعض الدول، لديها قوانين تنص على الاحتفاظ بأنواع معينة من البيانات، مثل البيانات الشخصية Les données personnelles، فى حوزة طوائف معينة من الحائزين، على أن يتم محوها Effacées إذا لم يعد فى الاحتفاظ بها ما يحقق فائدة تجارية.

وفى الاتحاد الأوروبى، القاعدة العامة هى ما ينص عليه الأمر95/46/EC، وفى السياق الخاص بقطاع الاتصالات الأمر 97/66/EC. وهذان الأمران ينصان على الإلتزام بمحو البيانات L'obligation d'effacer les données منذ أن يصبح تخزينها ليست له ضرورة Dès que leur stockage n'est plus né- cessaire واستثناء من هذه القاعدة، فإن الدول الأعضاء بمقدورها أن تتبنى تشريعاً يقرر استثناءات إذا كانت ضرورية من أجل منع ارتكاب الجرائم الجنائية Pour prévenir la commission d'infraction pénale أو التحقيق فى الجرائم Instruirec les infractions أو ملاحقة مرتكبها Pour suivre leurs auteurs بيد أن هذين الأمرين لا يمنعان دول الاتحاد الأوروبى من تأسيس أو إنشاء Instaur- ers سلطات Des pouvoirs وإجراءات Procédures فى القانون الداخلى من أجل التحفظ على بيانات معينة Pour conserver des données تعرض تنقيبات أو تحقيقات معينة.

وبالنسبة لغالبية الدول، فإن التحفظ على البيانات La conservation des données يعد سلطة Un pouvoir أو إجراء قانونياً Une procédure juridique جديداً كلية Entièrement nouveau فى القانون الداخلى. فهو أداة جديدة للتنقيب الهام فى مجال الكفاح ضد الإجرام المعلوماتى والجرائم المتصلة به، وبالأخص ضد الجرائم المرتكبة بواسطة شبكة الإنترنت وذلك للأسباب التالية:

أولاً: سرعة تغاير بيانات الحاسوب، قابلية البيانات المعلوماتية للتلاشي Vol-atilité، فإن هذه البيانات من السهل أن تخضع للتلاعب Manipuler أو التغيير Modifier وهكذا يسهل فقدان عناصر إثبات الجريمة، من خلال الإهمال وممارسات التخزين غير الدقيقة، أو التغيير العمدى لها أو محوها من أجل تدمير كل عنصر للإثبات Pour détruire tout élément de preuve، أو محوه في إطار العمليات العادية أو الروتينية لمحو البيانات التي لم تعد حاجة إليها. وإحدى وسائل المحافظة على سلامة البيانات De préserver l'inégrité des données تتمثل في قيام السلطات المختصة بعمل تفتيشات à opérer des perquisitions أو الولوج A'accéder بطريقة أخرى للبيانات لضبطها a'saisir أو الحصول عليها بطريقة أخرى.

ومع ذلك إذا كان حارس البيانات Le gardien des données جديراً بالثقة Est digne de confiance، كما في حالة شركة تجارية ذات سمعة طيبة Une bonne réputation، فإن سلامة البيانات يمكن ضمانها بطريقة أسرع عن طريق اصدار أمر بالتحفظ على البيانات Une injonction de conserver les don-nées[1] لديه. وبهذا يمكن أن يكون الأمر بالتحفظ على البيانات أقل قلقاً أو إخلالاً بالنظام بالنسبة للأنشطة، être moins perturbatrice وأقل ضرراً Moins préjudiciable على سمعة الشركة الأمينة à la réputation d'une entreprise honnête، من عملية تفتيش الأماكن بغرض الضبط.

ثانياً: تحديد هوية مرتكب الجرائم المعلوماتية: الجرائم المعلوماتية والجرائم المتصلة بالحاسب، غالباً ما يتم ارتكابها عن طريق نقل الاتصالات La trans-mission de communications[2] بواسطة نظام معلوماتي. هذه الاتصالات يمكن أن تحوى محتوى غير مشروع Un contenu illicite، مثال ذلك مواد

---

(١) ويقابل ذلك في المصطلح الإنجليزي An order to preserve tha data.

(٢) ويقابل ذلك في المصطلح الإنجليزي The Transmission of communications.

إباحية طفولية La pornographie enfantine⁽¹⁾، فيروسات معلوماتية Des virus informatiques، أو أية تعليمـــات Instructions أخـرى، تحـمل اعـتـداء على البـيـانات، أو تعـوق حـسن أداء Entravent le bon fonctionnemt⁽²⁾ النظام المعلومات، كما يمكن أيضاً أن تحوى عناصر Des eléments يمكن من خلالها إثبات أن جرائم أخرى قد تم ارتكابها، مثال ذلك حالات الاتجار بالمخدرات Des cas de trafic de stupéfiants أو النصب D'escroquerie وترتيباً على ذلك فإن التـحـقق من هوية مـصـدر أو منتـهـى La source ou de la destination هـذه الاتصالات الخارجـية يمكن أن يساعد على تحـديد هويـة مـرتكب هذه الجـرائم L'identilé des auteurs de ces infractions. ومن أجل تعيين مصدر ومنتهى هذه الاتصالات، ينبغى تجهيز أو تهيئة بيانات التجارة غير المشروعة المتعلقة بهذه الاتصالات الخارجية.

**ثالثاً: دور الاتصالات في كشف الجرائم التي تمت من خلالها:** عندما تقدم الاتصالات محتوى غير مشروع Un contenu illicite أو دليل أفعال جنائية La preuve d'agissements criminels، فـإن صـوراً Des copies مـن هـذه الاتصالات يتم الاحتفاظ بها بواسطة مقدمـى الخدمات Les fournisseurs de services، على سبيل المثال البريد الإليكترونى Courrier électronique التحفظ على هذه الاتصالات يكون هاماً من أجل عدم فقد عناصر الإثبات الجوهرية. فلا مراء فى أن إعطاء صور من هذه الاتصالات الخارجية، على سبيل المثال البـريد المخـزّن Courriers stockés، يمكن أن يكشف عن الجـــرائم التى تم ارتكابها.

إن سلطة التحفظ العاجل على البيانات المعلوماتية Le pouvoir de conservation rapide des données informatique يجب أن تسمح بمواجـهـة هذه

---

(١) ويقابل ذلك فى المصطلح الإنجليزى Child pornography.

(٢) ويقابل ذلك فى الطبعة الإنجليزية The proper functioning of the computer system.

المشكلات. وبالتالى يجب على الأطراف إنشاء أو تأسيس سلطة للأمر بالتحفظ على بيانات معلوماتية معينة. وبما أن هذا الإجراء وقتى Mesure provisoire، فإن الفترة الزمنية التى يتم فيها التحفظ على البيانات محددة زمنياً بحد أقصى ٩٠ يوماً، ويمكن للأطراف أن يقرروا تجديد Renouvellement هذا الإجراء.

هذا مع ملاحظة أن البيانات المتحفظ عليها، لا يتم الكشف عنها آلياً للسلطات القسرية Ne sont pas automatiquement. فلكى يحدث ذلك يجب اتخاذ إجراء إضافى Une mesure supplémentaire أو أمر بالتفتيش Ordonner une perquisition(*).

---

(*) من المهم أن توجد إجراءات للتحفظ على المستوى المحلى تسمح للأطراف أن يقدموا المساعدة على المستوى الدولى، فيما يتعلق بالتحفظ العاجل على البيانات المخزنة داخل حدودهم Sur leur territoire. ولا مراء فى أن هذا سوف يساعد على ضمان أن البيانات الجوهرية لا تختفىDisparaissent خلال الإجراءات المطولة لطلب المساعدة القضائية المتبادلة D'entraide judiciaire أثناء قيام الطرف المقدم إليه الطلب La Partie requise من الحصول على البيانات وإرسالها إلى الطرف مقدم الطلب أو (الملتمس) La Partie requérante.

الفصل الثاني

# الحماية الفنية للمعلوماتية

- التعريف بالأمن المعلوماتي.
- البُعد الاستراتيجي لأمن المعلومات.

● المبحث الأول: وسائل أختراق نظم الأمن المعلوماتي.

المطلب الأول: أهم وسائل أختراق نظم أمن المعلوماتية.

المطلب الثاني: تطبيقات عملية لأختراق نظم أمن المعلوماتية.

● المبحث الثاني: وسائل حماية المعلوماتية.

المطلب الأول: الوسائل القانونية.

المطلب الثاني: الوسائل الفنية.

المطلب الثالث: الوسائل الدولية.

# الفصل الثاني

# الحماية الفنية للمعلوماتية

**تمهيد:**

مع إدراك خطورة وسهولة ارتكاب أشكال الإجرام الجديدة التى أفرزتها بيئة المعالجة الآلية للبيانات(*)، والتنبه لآثارها السلبية على جهود التنمية الإدرية والاجتماعية، والاقتصاد والأمن الوطنيين، بدأت مكافحتها تحظى باهتمام متزايد من الحكومات وعدة منظمات دولية(**)، وأخذ الفنيون وخبراء أمن الحاسبات والنظم المعلوماتية، فضلاً عن رجال الصناعة(***)، يركزون جهودهم

---

(*) من مؤشرات ونتائج تزايد هذا الإدراك تنامي حجم المبيعات المتعلقة بأمن المعلومات والحاسبات. وقد بلغ حجم المبيعات المتعلقة بأولهما (أمن المعلومات) داخل U.S.A – على سبيل المثال – ٤ بليون $ سنة ١٩٨٨ وفقاً لدراسة أجراها اتحاد الصناعات الاليكترونية (EIA) – لا شك أنها زادت اضعافاً فى الوقت الحالى – فى هذه الفترة. وجاء بتقرير أخر أن سوق أمن الحاسبات قد بلغ إجمالى مبيعاته ٣,٨ بليون $ سنة ١٩٨٧. وأكدت تقارير أخرى أن سوق أمن المعلومات ينمو بنسبة ٢٠٪ تقريباً فى السنة، بينما ينمو سوق الحاسبات عامة بنسبة ٤٪ فقط فى السنة.

- Charles Cresson wood, Fifteen Major Forces Driving the civlian Information security Market, computers & security, vol. 9, No, 8. 1990, p, 679.

مشار إليه لدى د/ هشام رستم – مرجع سابق – هامش ٤ – ص ص ١٢، ١٣.

(**) مثل منظمة التعاون الاقتصادى والتنمية (O.C.D.E)، والسوق الأوروبية المشتركة (C.E.E.) ومجلس أوروبا (Conseil de L'Europe).

(***) وهؤلاء مع مديرى أمن نظم المعلومات، يميلون كما لاحظ البعض إلى تحميل القائمين على تنفيذ القانون، مسئولية الإخفاق فى وضع وتطبيق الوسائل والتدابير الفعالة التى تكفل مكافحة الأشكال الجديدة للإجرام التى أفرزتها تقنيات المعلومات. ولا يخفى الأخيرون شكواهم من أن الجرائم التى ترتكب بواسطة الحاسب – التى يقدمون بشأنها تقارير – ينتهى المطاف بمعظمها دون أن ينال الجانى عقاب، وأن القائمين على تنفيذ القانون يفتقرون إلى المهارات العالية فى هذا المجال وتتسم إجراءاتهم بالبطئ الشديد.

- Michael Alexander, computer crime: Ugly secret for business, computer world, vol. XXIV, No. 11, March 21, 1990, p. 104.

–/–

البحثية وتجاربهم العملية على سد ثغرات الأنظمة الأمنية، وتحسين وتطوير أساليب الحماية الفنية للنظم والبرامج والمعلومات، لتصل إلى أقصى درجة ممكنة من الفاعلية، دونما إنكار من جانبهم للحاجة إلى القانون لا سباغ صفة عدم المشروعية على انتهاك أمن منظومات المعالجة الآلية للبيانات، وتحديد إطار رد الفعل الاجتماعي تجاهه، وبالتالي تعزيز هذه الحماية الفنية.

والملاحظ أن طرق وأساليب الحماية الفنية الموجودة – حتى الآن – لا تكفل الآمن بصورة كاملة – مطلقة – للبيانات المخزنة في الحاسبات التي ترتبط عن طريق شبكات الإتصال ببعضها، أو التي يجري عبر هذه الشبكات نقلها. وكلما أحرزت أساليب الحماية تقدماً، فإن وسائل اختراقها تتقدم هي الأخرى بدورها، لأن عصر الحاسبات والمعلومات في سباقه مع الزمن يسير إلى كل جديد مفيداً كان أم مدمراً في الوقت نفسه.

والسائد بين خبراء أمن النظم المعلوماتية أن التكلفة الاقتصادية الباهظة للأساليب الفنية، التي يمكن أن تؤمن حماية كامة للأنظمة هي التي تحول دون استخدامها، وفيما دونها فإن أي نظام أمني يضرب حولها، يمكن لأي شخص يمتلك المعرفة والتصميم على بذل الوقت والجهد الكاف أن يخترقه(١).

وفي خضم شحذ الجهود والعقول لمواجهة خطر الإجرام المعلوماتي La criminalité informatique، ذهب رأي(٢) – بحق – إلى أنه من الضروري

---

-- تعليق: مع التسليم بوجاهة هذا الرأي فيما ذهب إليه، إلا أنه يفتقر إلى الموضوعية لأن القائم على تنفيذ القانون يلتزم بنصوصه ونظامه العقابي الذي أقره المشرع، وفي عدم التزامه مخالفة لقاعدة احترام الشرعية القانونية، ولا دخل في ذلك بالمهارة أو التفوق. كما وأن الاجراءات التي يطبقها القائم على تنفيذ القانون – مأمور الضبط القضائي – هي ما نص عليها القانون، فنعتها بالبطء الشديد لا يستقيم وشرعيتها.

(١) د/ هشام رستم – المرجع السابق – هامش ٣ – ص ١٣.

(٢) رأي د/ هشام رستم – المرجع السابق – ص ١٥.

* وفي معرض التدليل على مخاطر المعلوماتية على السيادة الوطنية ذكر قول القاضي الفرنسي لويس جوانيه (Louis Joinet) بعد إعلانه أن:

-/-

التصدى لبوادر هذا الإجرام التى بدأت تتبدى كى لا تستفحل مع وتيرة النمو

--- «المعلومات قوة. والمعلومات الاقتصادية قوة اقتصادية». إن «للمعلومات قيمة اقتصادية، والقدرة على تخزين أنواع معينة من البيانات ومعالجتها يمكن أن تعطى بلداً ميزات سياسية وتكنولوجية على البلدان الأخرى، وهو ما قد يؤدى إلى فقدان السيادة الوطنية لتلك البلدان من خلال انتقال البيانات فيما بين الدول».

ذكر هذا القول عن Louis Joinet فى مرجع:

Christopher J. Millard, Legal Protection: of Programs and Data, Sweet & Max Well Limited, London, 1985, p. 212.

ويضيف د/ هشام رستم عن قوة المعلومات وأهمية التقنية المعلوماتية:

ولدورها فى بسط النفوذ والهيمنة، تنظر دول العالم الثالث إلى تقنية المعلومات - بوجه عام - باعتبارها شكلا للأمبريالية التقنية Techno - imperialisme ، وضرباً من ضروب الاستعمار الجديد Neo colonialisme.

- Paul F. Burton, Information technology and organisation stnucture, Aslib proceedings, Vol. 40, No, 3, 1988. p. 59.

- وعلى الرغم من زيادة معدل التقنية للنظم المعلوماتية، إلا أن ذلك لا يضمن لها نظام أمن معلوماتى كافى، أو حتى حماية الكترونية بنسبة مطمئنة للمشروعات الحيوية حيث أكد أحد الباحثين الأمريكيين فى مجال الحماية الالكترونية، أن مجرمى الإنترنت أكتشفوا ثغرة أمنية خطيرة بالأنظمة الرئيسية التى تتحكم فى عدد من المؤسسات الحيوية، والتى تشمل مصافى البترول ومحطات توليد الكهرباء والمصانع. وأوضح الباحث أن تلك الثغرة يمكن استخدامها فى التحكم بالأنظمة الرئيسية لعدد من المؤسسات الكبرى التى تستخدمها، مثل أنابيب البترول والغاز ومحطات معالجة المياه وأجهزة التحكم بالكهرباء، فضلاً عن عدد من المصانع العملاقة التى تتبع كبرى شركات التكنولوجيا. وأضاف أن تلك الثغرة يمكن استغلالها فى اختراق عدد من الأنظمة الرئيسية للحاسبات وخاصة القديمة منها، إلا أن المشكلة تكمن فى أن تلك الأنظمة يتم استخدامها فى المؤسسات التى تمس الحياة اليومية للإنسان، الأمر الذى يشكل خطورة بالغة فى حالة اختراقها. (خاص من لاس فيجاس للأخبار - العدد ١٧٢٨١ - ٢٠٠٧/٩/٩ - ص ١٨ عالم المعلومات والأنترنت).

- وفى ذات السياق أظهر تقرير أمريكى جديد أن فيروسات الحاسبات وملفات التجسس كبدتا المواطنين خسائر بلغت حوالى سبعة مليارات دولار خلال العامين الماضيين. وأوضح تقرير (حالة الأنترنت) الذى أصدرته مؤسسة (كونسيومر ريبورت) الأمريكية من خلال استطلاع للرأى أجرته على عينة عشوائية شملت ألفى أسرة، أن مستخدمى الأنترنت فى البلاد معروضون لهجمات مجرمى الإنترنت بنسبة ٢٥٪. وأكد ٣٨٪ من جملة عدد المشاركين فى الاستقصاء تعرض أجهزتهم للأصابة بالفيروسات الالكترونية خلال تلك الفترة، فيما عانى ٣٤٪ منهم من ملفات التجنس الالكترونية والتى تم تحميلها على أجهزتهم عبر الانترنت. (ذات المصدر - ص ١٨).

المتسارع، الذى تشهده دول عربية عدة – فى استخدام النظم المعلوماتية – وما تهيئة أوضاع نظم الحكم فى بعضها. فضلاً عن ظروف السياسة الدولية والتبعية التكنولوجية، وارتفاع نسبة العمالة الأجنبية فى قطاع المعلوماتية، من مناخ موات لانتهاك حرمة البيانات الشخصية، وحق الإنسان فى الخصوصية، والمساس بالأمن القومى لهذه الدول وسيادتها الوطنية.

وعلى هذا الأساس، سوف تنقسم دراستنا لهذا الجزء الهام من البحث (الحماية الفنية للمعلوماتية) إلى مبحثين بيانهما:

**المبحث الأول: وسائل أختراق نظم الأمن المعلوماتي:**

ويتم عرض هذا الوسائل فى المطلب الأول، ويلى ذلك بيان لبعض التطبيقات العملية والقضايا الهامة التى استهدف اختراق نظم أمن المعلومات فى المطلب الثانى.

**المبحث الثاني: وسائل حماية المعلوماتية:**

وتشمل هذه الوسائل ما يلى:

المطلب الأول: الوسائل القانونية لحماية المعلوماتية.

المطلب الثانى: الوسائل الفنية لحماية المعلوماتية.

المطلب الثالث: الوسائل الدولية لحماية المعلوماتية.

ويسبق هذا العرض ايضاح للبُعد الاستراتيجى لأمن المعلومات، على مستوى المؤسسات والكيانات الاقتصادية الكبرى، ثم على مستوى الدول والكيانات السياسية القائمة، بعد تستطير مفهوم الأمن المعلوماتى بالتعريف بمعناه من خلال عرض ماهية أمن المعلومات ومستويات ومجالات الأمن المعلوماتى.

## أولاً: التعريف بالأمن المعلوماتي:

لعبت المعلومات الركيزة الأساسية في رقى وتقدم المجتمعات بل أضحت المعلومات هي المحك أو المحور الرئيسي في بقاء واستمرار أي منشأة، لذلك شكلت معضلة الأمن والحماية الدورية والكافية لتلك المعلومات الشغل الشاغل والقضية الأهم لكل مسئول عن كيان أو منشأة ما، أمن يكفل لنظام المعلومات الحماية والبقاء وفي ذات الوقت القيام بوظائفه الأساسية دون صعوبات أو تعقيدات، مع مراعاة تحقيق التوازن المطلوب دائماً بين التقدم التكنولوجي المستهدف لنظم المعلومات والخصوصية الشخصية الواجبة، فالمسافة المتاحة للخصوصية تتناسب عكسياً.. مع التقدم التكنولوجي لنظم المعلومات والاتصالات[1].

### أ - ماهية أمن المعلومات[2]:

أمن المعلومات هو حماية أصول وموارد ومكتسبات نظام معلوماتي ما بطرق مشروعة، وهو أيضا أداة تتحكم في تنظيم العلاقات والاتصالات، وذلك دون أن يؤثر على قدرة مستخدمي هذا النظام على الأداء أو يعوق عملهم من حيث الكفاءة أو التوقيت، وهذا الأمن المعلوماتي لا يمنع الجريمة المعلوماتية كلياً، ولكنه كلما كان قوياً ودقيقاً وفاعلاً، كان من الصعب ممارسة الاختراق ضد نظام المعلومات المستهدف، وإن تحقق ذلك، فإن فعل الأختراق والإجرام المعلوماتي إما أن يكون:

أ – مرهقاً للقائم على تلك الجريمة.

ب– مكلفاً ويتساوى أو يقارب مع الهدف المبتغى من الاختراق.

جـ– يستغرق وقتاً طويلاً للنجاح.

د – يسهل اكتشافه قبل النجاح فيه أو بعده.

لذلك كان الحرص على وجود عملية فعالة لأمن المعلومات، هو إجراء يتم بصورة تلقائية أو عفوية من القائمين عليه، منذ بدء التعامل أو الاستخدام الفعلي

(١) لواء د/ محمود وهيب السيد – مفاهيم أساسية في أمن المعلومات – مرجع سابق – ص ٢٧.

(٢) المرجع ذاته.

لنظم المعلومات، سواء أكانت هذه النظم نظاماً بدائياً يعتمد على الأقلام والأوراق والدفاتر، أو نظاماً حديثاً يقوم بالأساس على الأجهزة الحاسبة ونظم المعلومات المعتمدة عليها، رغم حقيقة أن مصطلح أمن المعلومات لم يظهر على السطح الأكاديمي إلا بعد شيوع انتشار نظم المعلومات بالمعنى أو وفق التطور الأخير، حيث انتشر بشكل كبير وواسع ما يعرف بشبكات المعلومات بأنواعها الثلاث: الداخلية أو المحلية Lan. والخارجية أو الدولية Wan، والشبكات الخاصة مثل In-ternet، وهذا ركن هام يدفعنا لعرض الجانب التالي:

**ب- مستويات الأمن المعلوماتي(١):**

**ومستويات الأمن تتعدد وتتنوع بحسب وجهات النظر التالية:**

* إذا صنف مستوى الأمن حسب درجة السرية القائمة، فنكون أمام المستويات التالية:

إذا كان الأمن المستهدف لنظم المعلومات أمناً كلياً، كانت درجة السرية المطلوبة سري للغاية.

إذا كان الأمن المستهدف لنظم المعلومات أمناً جزئياً، كانت درجة السرية المستهدفة درجة سري.

إذا كان الأمن المستهدف لنظم المعلومات أمناً مناسباً، كانت درجة السرية المستهدفة درجة هام فقط.

** أما إذا صنف مستوى الأمن حسب الإجراءات المتبعة، فنكون أمام المستويات التالية:

إذا كانت عمليات الأمن المطلوبة وقائية، كانت الإجراءات المتبعة تستهدف منع الأخطاء المتعمدة أو غير المتعمدة.

---

(١) - المرجع ذاته - ص ٢٨.

إذا كانت عمليات الأمن المطلوبة ثابتة، كانت الإجراءات المتبعة تستهدف تحقيق الدفاع عن النظام المعلوماتى، بتأخير عمليات الاختراق ورفع تكلفته.

إذا كانت عمليات الأمن المطلوبة متحركة، كانت الإجراءات المتبعة تستهدف تحقيق الدفاع عن النظام المعلوماتى، بوسائل تتعامل مع المخترق ذاته.

**جـ- وإذا كان التصنيف نوعياً فتكون الإجراءات المتبعة علي النحو التالي:**

تستخدم وسائل طبيعية للأمن، حينما يكون الأمن طبيعياً أى عندما يقل إحتمال وصول مستخدم غير قانونى، والوسائل الطبيعية للأمن تستهدف بالأساس منع الاختراق الطبيعى.

تستخدم وسائل صناعية للأمن، حينما يكون الأمن صناعياً أى عندما يزيد احتمال وصول مستخدم غير قانونى، والوسائل الصناعية للأمن تستهدف بالأساس استخدام وسائل صناعية إضافية لمنع أو تنظيم الوصول عن بعد.

تستخدم وسائل مختلطة للأمن، حينما تتساوى الاحتمالات، والوسائل المختلطة للأمن تستهدف استخدام كلا الوسيلتين الطبيعية والصناعية.

وهناك بالطبع مستويات أو أنواع أخرى لتصنيف الأمن المعلوماتى، فقد يكون المستوى المطلوب للأمن مستوى شمولياً، وقد يكون المطلوب أمناً محكماً لا يمكن اختراقه، وقد يكون ذا مستوى للجودة بالقياس لمعيارية ما، أو غير ذلك من التصنيفات المختلفة.

**د - مجالات الأمن المرتبط بالمعلومات[1]:**

هناك أنواع عدة ومجالات متنوعة للأمن المرتبط بنظم المعلومات، نذكر منها:

**- أمن المعلومات Information Security:**

وهو المرتبط بالمعلومات التى هى أساس أو هدف نظام المعلومات القائم

(١) المرجع ذاته – ص ٣٠.

والذى يشكل عصب أو حياة المنشأة الحديثة، وهو يعمل على حماية المعلومات ذاتها، وأيضاً العمل وبذات الدرجة على حماية مخازن المعلومات بمعناها الفنى أو الاصطلاحى الحديث.

- أمن الوصول إلي الأنظمة Access Control:

وهو يعنى بعملية التأمين المعلوماتى، المرتبطة بالأساس بعمليات التعامل مع البيانات والمعلومات القائم عليها نظام المعلومات بالمنشأة، وتشمل تلك الإجراءات تأمين أو عمليات التحكم فى الدخول لنظام المعلومات ذاته، والتحكم فى التطبيقات التى يعمل عليها نظام المعلومات بالمنشأة، وهو غالباً ما يكون على عدة مستويات طبقاً للمستوى الوظيفى لمستخدم هذا النظام، ودرجة احتياجه للمعلومات المراد التعامل معها، بالنسبة لتخصصه الوظيفى أو للصلاحية الشرعية المسموحة بالمنشأة.

- أمن برمجيات نظم المعلومات Software Security:

وهى العملية التى تستهدف حماية البرامج التى تشغل أو يقوم عليها نظام المعلومات ذاته، وهى البرامج التى تحدد مسار البيانات وكيفية التعامل معها والمعلومات بالمنشأة وكيفية الاستفادة منها وتوظيفها، وهى تشمل عمليات التأمين ضد أعمال القرصنة، والتأمين ضد السطو عليها من الخارج أو الداخل، أو أعمال التخريب أو الإتلاف المتعمد لها.

- أمن الاتصالات Communications Security:

وهى عمليات تأمين وسائل الاتصال التى تعتمد عليها المنشأة فى أعمالها الوظيفية، وتشمل تأمين وسائل الاتصال السلكى من خطوط تليفونية وخطوط ومسارات كوابل نقل المكالمات وأجهزة نقل وتداول الاتصالات. وأيضاً محطات الاتصالات المركزية أو الرئيسية الداعمة أو المقوية للاتصالات التليفونية، كما تشمل عمليات التأمين وسائل الاتصال اللاسلكى، سواءً أكانت وسائل إتصال لاسلكى مستقل، أو وسائل اتصال لاسلكى ملحقة بأجهزة أخرى.

### ثانياً: البعد الاستراتيجي لأمن المعلومات:

في الوقت المعلوماتي الحاضر، زادت عمليات اختراق نظم المعلومات ذات البُعد الاستراتيجي (العسكري والاقتصادي والعلمي)، وتعرضت هذه المراكز لاعمال القرصنة المعلوماتية من أجل الحصول على البيانات والمعلومات المتداولة أو المخزنة في ذاكرة الحاسبات الآلية(*).

وعمليات اختراق نظم المعلومات والتي تهدد الأمن القومي ليست قاصرة على دولة بعينها، فكما وقعت في الولايات المتحدة الأمريكية، وقعت كذلك في دولة الإمارات العربية المتحدة، وجمهورية الصين، واستهدفت العراق رغم تدمير بنيته التحتية، بما فيها من شبكة الاتصالات، وامتدت إلى اليابان وكندا، وبلدان غربية أخرى عديدة(**).

---

(*) نستطيع أن نقول أنه قد اختلف اختراق المؤسسات وأنظمة المعلومات للدول عن ذي قبل، فقد تكونت في الدول الكبرى ذات المصالح المتعددة على مستوى دول العالم - أمريكا وبعض دول أوروبا - منظمات تخصصت في اختراق شبكات الكمبيوتر، تعمل معظم هذه المنظمات بشكل شرعي وقانوني وتعاون مع الجهات الأمنية الفيدرالية في أمريكا، لتنظيم العمل نحو اختراق شبكات المعلومات للدول التي تعارض سياسة شرطي العالم. وهم في ذلك يختفون تحت عباءة شعار الدفاع عن حقوق الإنسان والتصدي للأضطهاد. د/ عبد الفتاح بيومي حجازي - الأحداث والإنترنت - دار الفكر الجامعي - الاسكندرية - سنة ٢٠٠٤ - ص ٢٢٦، وأيضاً يراجع: عبد القادر الكاملي - تقرير بعنوان التجسس عبر الإنترنت وحروب الشبكات - مجلة إنترنت العالم العربي - موقع شبكة Ditnet. وعنوانها: http: // www. ditnet. co. ae.

(**) قام مكتب التحقيقات الفيدرالية الأمريكي بالقبض على شاب - دون الثامنة عشر - في قضية تجسس اليكتروني يدعى - شامليون Chameleon - حيث كان المحققون يشكون في تورط الشاب في بيع أسرار عسكرية لآخر يدعى - خالد ابراهيم - عضو في جماعة هندية تسمى - حركة الأنصار - وهي مصنفة من قبل السلطات الأمريكية بوصفها من المجموعات الإرهابية، والمطلوب كان معلومات عن إدارة معدات شبكة نظم المعلومات بوزارة الدفاع الأمريكية (DEM) عام ٢٠٠٠ (عبد القادر الكاملي - تقرير بعنوان التجسس عبر الإنترنت وحروب الشبكات - مجلة إنترنت العالم العربي - مصدر سابق).

- كما تمكنت مجموعة أمريكية من اختراق - ستة جدر من جدران النار Firewalls - نظم أمن معلومات صينية بهدف منع الصينيين من استقبال معلومات ممنوعة من باقي بلدان العالم، ووجهت النظام كي يتجاهل أوامر المنع، ويسمح لمستخدمي الانترنت بزيارة أي موقع على

-/-

١ - في أطار أمن المؤسسات القومية:

بدأت محاولات اختراق النظم الأمنية للمعلوماتية منذ سنوات ماضية، وقد استهدفت شركات الكومبيوتر والجامعات ومكتب التحقيقات الأمريكي، والبنتاجون، ووكالة الفضاء الأمريكية ... وغير ذلك من المؤسسات ذات الصبغة القومية، لكن معظم هذه المحاولات كانت فردية، ينفذها هاكرز للحصول على أسرار تقنية تعود عليهم باستفادة مادية. أو لتنفيذ عمل تخريبي بلا هاوية محددة.

تمكن طالب جامعي - جيسون - يدرس في قسم علوم الكمبيوتر، من اختراق شبكة وكالة الفضاء الأمريكية (ناسا)، بهدف التعرف على النظام الأمني الذى تتبعه فى الحماية. وما فعله هذا الشاب - ٢٢ عام - يكاد يكون المستحيل ذاته، وذلك لوجود برامج معقدة تجعل من الشبكة بمثابة قلعة حصينة لكنه تفرغ لهذه المهمة وأنجزها(*).

- وفور حصول عملية الاختراق، استنفرت أجهزة الأمن فى وكالة - ناسا - بعد اكتشاف عملية الاختراق والذى خلف تدميراً فى الملفات قدرت قيمته بحوالى

= الشبكة، ثم قاموا بالدخول إلى شبكة معلومات مدينة - تيان جين - للعلوم والتقنية وأحدثوا تلفاً وتخزيباً فى الموقع. (عبد القادر الكاملى - التجسس عبر الانترنت - مرجع سابق).

- وفى دولة الإمارات العربية المتحدة - يونيو ٢٠٠٠ - تمكن أوروبيا من اختراق - شبكة - نظم اتصالات، وتخريب الإنترنت بها، وقد القى القبض عليه والتحقيق معه، وتبين أنه بريطانى الجنسية، وقد تسبب فى إصابة شبكة المعلومات - الانترنت - بالشلل لمدة أسبوعين بسبب اعمال التخريب التى قام بها. (د/ عبد الفتاح بيومى حجازى - المرجع السابق - ص ٢٢٩).

- وفى هولندا - حال غزو العراق لدولة الكويت - تمكن أحد القراصنة من سرقة أسرار عسكرية أمريكية بالغة الخطورة، عن تحركات القوات الأمريكية ومواقعها وأسلحتها وتحركات الطائرات المقاتلة، وأرسل القرصان هذه المعلومات إلى العراق قبل اندلاع الحرب، لكن لم يستفيد العراق من هذه المعلومات. (د/ جميل عبد الباقى الصغير - الإنترنت والقانون الجنائى - مرجع سابق - ص ٣٤).

(*) راجع تحت عنوان - قصص إنترنت (إختراق حصن وكالة الفضاء الأمريكية) - إعداد فاطمة نعناع، مجلة إنترنت الوطن العربى على موقع http:// www. dit-net co. ae.

سبعين ألف دولار، بالإضافة إلى إضطرار الوكالة لتغيير النظام الأمنى لموقعها على الشبكة، حيث رفعت «ناسا» الأمر إلى مكتب التحقيقات الفيدرالى (FBI) الذى بدأ تحقيقاته بفحص سجلات الدخول إلى الشبكة، فى الفترة التى تم اختراق الموقع خلالها، وتمكن المكتب من التعرف على رقم (ip) للكومبيوتر الذى قام بهذا الفعل، وأظهر هذا الرقم أن الاتصال تم عن طريق مؤسسة تقدم خدمات إنترنت فى مدينة تقع شمال «أونتاريو» فى كندا، وليس فى الولايات المتحدة الأمريكية.

– وقد استعان مكتب التحقيقات الفيدرالية بالشرطة الكندية الملكية، وقدم لها المعلومات التى فى حوزته مثل رقم (ip) الخاص بالكومبيوتر المتصل، والزمن الذى تم فيه الاتصال.

– وقد بدأت الشرطة الكندية مهمتها بالاتصال مع مؤسسة خدمات أنترنت، وحصلت على اسم المشترك الذى يعود إليه رقم (ip) المذكور. وبدأت التحقيق معه، وتبين لها من خلال أدلة واضحة عدم قيامه بمثل هذا الفعل. وقد توصلت الشرطة الكندية إلى أن الفاعل لابد وأن يكون قد حصل – بطريقة غير مشروعة – على رقم المرور السرى لذلك المشترك وأجرى الاتصال عن طريقه.

– وحاولت الشرطة كذلك التدخل إلى الفاعل عن طريق رقم الهاتف الذى انطلق منه الاعتداء، وتمكنت بالفعل من الوصول إلى هذا الرقم عن طريق الاستعانة بمؤسسة خدمات إنترنت التى تم الاختراق عن طريقها، وعن طريق مؤسسة الهاتف الكندية.

– وقد تبين للشرطة هناك أن الهاتف يعود إلى شخص يعمل مديراً لإحدى الشركات الكبرى، ولا تضم سجلاته أية سوابق بمثل هذه الأعمال أو غيرها، لكن التحريات، اثبتت وجود – جيسون – إبن المدير المذكور والذى يدرس علوم الكومبيوتر، وكان يتردد على منزل والده بصفة دائمة فى ذات الفترة التى تم

فيها اختراق موقع «ناسا»، ولذلك فهذا الابن هو النموذج المثالى المحتمل لمن قام بهذا الاختراق.

- وعندما قامت الشرطة بمهاجمة المنزل ضبطت جهازى كمبيوتر كان - جيسون - يستعملهما، بالإضافة إلى ضبط وثائق مهمة أكدت قيامه باختراق وكالة الفضاء الأمريكية - ناسا - والشئ الغريب أنه عند قيام الشرطة بمواجهته بما قام به، تبين أنه نسى ذلك الأمر والذى مضى عليه عدة أشهر[1].

- وقد أسفر اختراق المتهم المعلوماتى عن تدمير برامج قيمتها سبعون ألف دولار، فضلاً عن تغيير النظام الأمنى للوكالة كاملاً، الأمر الذى كلف الحكومة الأمريكية ملايين الدولارات.

= ولعل هذه الاختراقات هى ما دفعت المسئولين الأمريكيين إلى القول بأن عمليات تخريب الإنترنت تهدد الأمن القومى الأمريكى. وقد سارع الرئيس الأمريكى السابق - بيل كلينتون -فى حينه إلى تخصيص - مليارى - دولار للمواجهة أخطار اختراق شبكات الكومبيوتر الأمريكية بطريق الإنترنت[2].

- الأكثر من هذا أن هذه الاختراقات والتى قد تهدد الأمن القومى لدولة أو النظام الأمنى لمؤسسة أو كيان اقتصادى عملاق، قد لا تكون من محترفين بل من هواة، أحداث وشبات هدفهم إثبات قدراتهم - المعلوماتية الفائقة - وليس الحصول على هذه الأسرار من أجل بيعها وتسويقها تجارياً[3].

**ب- في أطار الأمن القومي:**

عمليات أختراق أمن المعلومات، تقوم بها الأفراد والجماعات، بل الدول

(١) راجع فاطمة نعناع، اختراق حصن وكالة الفضاء الأمريكية، مجلة إنرنت، عام ١٩٩٨، على موقع http: // news. bbc. co uk.

(٢) راجع: عمليات تخريب الإنترنت تهدد الأمن القومى الأمريكى على موقع http: // news. bbc. co. uk. بتاريخ ٢٠٠٠/٢/١٧.

(٣) راجع دراسة بعنوان - موقعك فى ويب - فى مهب الاختراق، إعداد فادى سالم، مجلة إنترنت العالم العربى على موقع: http: // www. iawnag. co. ae.

على نحو يهدد الأمن القومي، وحسب قدرات هذه الدول وتقدمها تكنولوجياً حتى أن بعض الباحثين والمتخصصين، وبسبب التبعية العربية المعلوماتية لشركات نظم وتقنية المعلومات الكبرى، يرون أن الأمن القومي في المجال المعلوماتي مخترقاً، وتحديداً من قبل اسرائيل، بسبب تفوق اسرائيل معلوماتياً، كما أن هذه الأنظمة تعتمد على حلول أمنية مصنعة في اسرائيل(١) .

---

(١) راجع فادى سالم، اختراق الأنظمة الحكومية العربية، على موقع http: // www. ditnet. co. ae.، مشار إليه لدى، د/ عبد الفتاح بيومى حجازى – مرجع سابق – سنة ٢٠٠٤ – ص ٢٣٨ وما بعدها.

- ويرجع التفوق المعلوماتي الاسرائيلي إلى أنها تلقت حوالى (٨٠٠) ألف مهاجر من الاتحاد السوفيتى السابق، وأدت هذه الهجرة إلى ارتفاع نسبة العلماء والمهندسين فيها حيث وصلت فى أواخر التسعينات إلى رقم قياسى عالمى هو (١٣٥) عالماً أو مهندساً لكل عشرة آلاف نسمة، وكان لهؤلاء دور بارز فى دفع عجلة الصناعة المعلوماتية، وفى ظل وجود تخطيط سليم للاستغلال الأمثل لهؤلاء العلماء كانت طفرة الصناعة المعلوماتية لديهم وجعل من اسرائيل قلعة متطورة على مستوى العالم فى صناعة المعلوماتية، ودفع كبرى شركات العالم للتهافت على اسرائيل والاستثمار فيها مادياً وبشرياً فى نطاق هذه الصناعة، وتخلص عوامل النجاح لهذه الصناعة المعلوماتية لديها فى الآتى:

أ – وجود الجامعات والمعاهد الفنية المتخصصة فى المعلوماتية، مثل معهد Technicon فى حيفا الذى قدم عقولاً متخصصة فى المعلوماتية، لدرجة أنه إخصائياً قيل بأن من قدمهم هذا المعهد فى ذلك المجال يعادلون من قدمتهم جامعة Standford ومعهد Mit فى الولايات المتحدة وذلك فى مجال صناعة المعلوماتية.

- ويقابل ذلك عندنا فى مصر وجود كليات ومعاهد متخصصة فى الحاسب الآلى، وإن اتجهت لها الأنظار مؤخراً، لكن المستقبل واعد بالنسبة لهذا الشباب المصرى والعربى فى ذات المجالات المماثلة، حيث بدأت الجامعات العربية تتجه نحو علوم الحاسب الآلى وهندسته وتطبيقاته فى محاولة لسد الفجوة التعليمية والتطبيقية في تكنولوجيا المعلومات بيننا وبين الدول المتقدمة.

ب – إعتماد خطط تجارية مبتكرة لدعم المشاريع المعلوماتية: فقد تنبه الخريجون الجدد فى المعاهد التقنية الاسرائيلية إلى عدم قدرتهم على منافسة الشركات الكبرى فى هذا المجال، فكونوا تجمعات من شركات صغيرة تتعاون مع شركات عالمية كبيرة وهو ما أدى إلى أن معظم الشركات العالمية تتعامل مع هذه الكيانات الاسرائيلية الصغيرة وتتعاون معها فى مجال تقنية المعلومات ومن هذه الشركات مايكروسوفت، إنتل، هيوليت باكارد، كومباك 3com, cisco, lucent, Aol, IBM, General electic, Computer Associates, Texas instruments, Motorolla, وشبكة Yahoo, Cnet، وغيرها من الشركات.

–/–

- ويرى خبراء نظم الحاسب الآلى والمعلومات، فى مسألة الأمن القومى

جـ- القوات المسلحة الاسرائيلية مدبع لخبراء أمن المعلومات، ذلك أن سنوات الخدمة العسكرية فى الجيش الاسرائيلى تختلف عنها فى الكثير من دول العالم، إذ أنها فترة لتطوير خبرات المختصين فى مجال أمن المعلومات.

- وهذا الأمر من أهم العوامل المؤثرة فى دفع تطوير الحلول الأمنية والتطبيقات المتعلقة بأمن المعلومات فى اسرائيل، ويكفى للعلم، إن شركة Check point الاسرائيلية، وهى تقدم أكثر حلول أمن المعلومات انتشاراً فى العالم، لدرجة أن حصتها فى سنة من السنوات وصلت إلى ٤٤٪ فى سوق الجدران النارية فى العالم، هى شركة طورها ضابط فى الجيش الاسرائيلى يدعى - شارون كارمل - مع بعض زملائه الذين قضى معهم خدمتهم الإلزامية فى الجيش لتطوير أنظمة - حاسب آلى - تحاكى أو تشبه ساحات القتال، وتطور وسائل ربط شبكات حاسب آلى عالية الأمان.

- ولهذا يرى رؤساء شركات أمن المعلومات الاسرائيلية أن مدة الخدمة الإلزامية للجندى الاسرائيلى وقدرها ثلاث سنوات تمكنه من التعرف على كثير من التقنيات الحديثة وتتيح له فرصة التعامل معها، وتشكل أساساً لعمليات إبتكار للتقنية الحديثة التى تأخذ طريقها للتوزيع التجارى.

- ولاشك أن أصحاب القرار فى الجيوش العربية مدعوون للأخذ بأسباب هذا التطور فى اعداد الجندى العربى المتعلم والمثقف والواعى بفنون وتقنيات العصر، وأن يترك الجنود ذوى الخبرات المحدودة أو المتوسطة للابداع فى مجالات أخرى كالزراعة والمهن الحرفية التى يجيدونها.

- ومن المجالات التى تفوقت فيها شركات المعلوماتية الاسرائيلية، مجال برامج أمن الشبكات كالجدران النارية، حيث لاحظ الوافدون الجدد إلى سوق المعلوماتية الاسرائيلية، أهمية أنظمة الشبكات وتطبيقات الإنترنت ومدى انتشارها، ولذلك فقد ركزوا على الانتاج فى هذا المجال، وظهرت شركات مثل Alladim و Check point التى قدمت منتجات عالمية.

- ولاحظوا كذلك أهمية التشفير فى عصر الإنترنت فأجريت دراسات عديدة فى هذا المجال وأدت إلى ظهور عدد من التقنيات العالمية مثل تقنية R.S.A الشهيرة للتشفير وتنتجها شركة بذات الاسم، وهى تستخدم فى كثير من مواقع التجارة الإليكترونية والتبادلات الإليكترونية فى الإنترنت.

د - الدعم الحكومى، حيث لاحظت الحكومة الاسرائيلية التطور الكبير فى ميدان تقنية المعلومات لديها وتدفق الشركات العالمية فى مجال تقنية المعلومات، ولذلك فقد رغبت فى الحصول على حصة فى الشركات الاسرائيلية العاملة فى هذا المجال، حيث زادت استثماراتها لدى الشركات الصغيرة فى هذا المجال بمقدار مليار دولار عام ١٩٩٨، كما أنها تخصص مبلغ - ٣ مليارات - دولار سنوياً للبحث العلمى.

- وهذه دعوة مفتوحة للحكومات العربية للانفاق بسخاء على تقنية المعلومات، لأن من يملكها اليوم له اليد العليا فى قراره وسيادته ومصيره ورفاهية شعبه، صحيح أن الحكومات تنفق على تقنية المعلومات، لكن الوصول إلى الوضع الأمثل يقتضى المزيد والمزيد من الانفاق لاسيما فى ظل وجود المال، وفى ظل تمتع الشعوب العربية بقدرات بشرية وعقلية هائلة.

-/-

العربى أن تبعية العرب فى مجال تكنولوجيا المعلومات، خاصة برامج الحماية لهذه النظم والتى تمتلكها شركات أجنبية ومنها شركات اسرائيلية أمر له خطورته، ويعرض الأمن القومى والعربى للخطر، ويضعه تحت سيطرة غربية بصرف النظر عما إذا كانت هذه الدول من الأعداء أم الأصدقاء فهى تتجسس على بعضها، بصرف النظر عن العلاقات بينها، وهذه حقيقة قائمة لا مفر منها، ولا يقتصر التجسس على الأهداف العسكرية فقط، بل يمتد كذلك إلى المجالات التجارية، ذلك أن الشركات العاملة فى مجال تقنية المعلومات تتجسّس على بعضها البعض مثلما فعلت شركة Real Networks وإنتل ومايكروسوفت وغيرها، بالإضافة إلى شبكات ومواقع إنترنت عديدة للحصول على معلومات تعطيها الأفضلية فى المنافسة، ولذلك فالسؤال المطروح هو ما الضمان فى عدم تجسس الشركات الاسرائيلية وغير الاسرائيلية والتى تقدم الحلول الأمنية لأمن البيانات بالنسبة لشبكات الدول العربية أو الأنظمة المعلوماتية التى تعتمد على هذه الحلول؟

– لذلك لابد من تطوير حلول أمن المعلومات محلياً، وكذلك وضع الحلول الأجنبية التى ترغب الدول العربية فى استخدامها تحت اختبارات مكثفة، ودراسات متعمقة للتأكد من خلوها من الأخطار الأمنية[1].

وأن يكون الإعتماد الأكبر على الخبرات الوطنية فى مجال نظم أمن المعلومات، ولا شك أن الوطن العربى لا ينضب من النماذج المتميزة فى المجال المعلوماتى، والمطلوب هو تهيئة المناخ المناسب لعمل وإنتاج هولاء.

---

– ولا يقتصر التفوق الاسرائيلى على مجال تقنية المعلومات فى مجال أمن المعلومات فقط، فهناك مجالات أخرى تتفوق فيها مثل التشفير، والتراسل الفورى، وتقنيات الصوت والفيديو، ومن أشهر برامج التاسل الفورى برنامج يسمى (icq) من شركة Mirabilis وبرنامج Gooey من شركة Hypernix الذى يتوقع له النجاح مثل برنامج icq.

راجع فى ذلك: فادى سالم، اختراق الأنظمة الحكومية العربية، مرجع سابق، على موقع: http: // www. ditnet. co. ae.

(١) فادى سالم، المرجع السابق، الموقع السابق على شبكة الإنترنت.

## المبحث الأول

## وسائل اختراق نظم الأمن المعلوماتي

تتوافر أكثر من وسيلة معلوماتية (برمجية) على عموم ساحة الحاسبات الآلية وشبكاتها، وشبكة الإنترنت، ومواقع الويب Web Sites، تحمل بين ثنايها مفتاحاً مهماً لتجاوز العقبات التي تعترض إدارة نظام الحماية، وضمان سلامة البيانات والنظم البرمجية كما أنها تتيح لهم إمكانية حل الرموز والشيفرات التي تعترض الأنشطة السائدة في ميدان أمن المعلومات(*).

ويصورة عامة يمكن تعريف الوسائل المعلوماتية التخريبية بأنها(١): عبارة عن برمجيات أو وسائط تقنية قابلة للتوظيف مع عتاد الحاسوب وبرمجياته لتحقيق الأهداف الرئيسة التالية:

١- مضايقة وإنهاكاً مستمراً لموارد النظام المعلوماتي.

٢- تدمير قواعد البيانات والمعارف، وموارد البرمجيات والنظم التطبيقية.

٣- إحداث ثغرات في النظام المعلوماتي، أو التمهيد لها من خلال الكشف عن مواطنها.

وتستغل هذه الأدوات من قبل قراصنة المعلومات لضمان سهولة اختراق الشبكات، عن طريق استثمار الإمكانيات المتاحة في هذه الأدوات للوقوف على

---

(*) مع تنامي التكنولوجيا الخاصة بالاتصالات، فإن الأخطار التي تهدد أمن المعلومات التي يجري تبادلها في تزايد مستمر، حيث يمكن لمحللي نظم الشبكات عرض المعلومات على شاشة الحاسب الآلي بسهولة، وكل من يريد الاطلاع على المعلومات، ما عليه سوى الدخول إلى الشبكة والتجسس على المشروعات الضخمة، والمواقع الشخصية وسرقة بياناتها، وذلك في امكان الأحداث، كما هو في مكنة الكبار المحترفين، ومن هنا يتعين تأمين قنوات الإتصال، عن طريق معدات تشفير متقدمة، تتولى تشفير الرسائل عند بثها وفك الشفرة عند استقبالها، وتحويل المعلومات والمناظر إلى أرقام حتى يمكن تشفيرها. راجع: د/ جميل عبد الباقي – الإنترنت والقانون الجنائي – مرجع سابق– ص ٤٦.

(١) أ/ حسن مظفر الرزو – مقالة بعنوان: الأمن المعلوماتي (معالجة قانونية أولية) – مجلة الأمن والقانون – أكاديمية الشرطة دبي – السنة الثانية عشر – العدد الأول – يناير ٢٠٠٤ – ص٧٠.

طبيعة الثغرات الأمنية الموجودة على الشبكة، والاستفادة منها لفك الرموز والشيفرات التى قد يصعب عليهم حلها بأدواتهم الشخصية.

## المطلب الأول

## أهم وسائل اختراق نظم أمن المعلوماتية

ومن أهم الوسائل المتاحة لاستخدامات انتهاك واختراق نظم الأمن المعلوماتى ما يلى(١):

**أولاً: الفاحص Scanner:**

يمكن تعريف الفاحص بأنه عبارة عن برنامج تطبيقى أعد لأغراض الكشف الآلى عن مواطن الضعف فى المضيفات المحلية والنائية Local & Remote Hosts. تعمد هذه البرمجيات إلى قرع أبواب طرفيات TCP/IP والخدمات المصاحبة لها، والتى تشمل مثلاً Telnet & FTP وتباشر بعملية تسجيل ردود أفعالها من الموقع الهدف.

وبذلك توفر هذه الأدوات معلومات ثمينة تخص الهدف المضيف ومستوى الحماية الأمنية المعلوماتية التى يمتلكها. من أجل هذا تتبوأ هذه الأداة مكانة متميزة فى ميدان أمنية شبكة الانترنت، وتعتبر مورداً ثرياً لقراصنة المعلومات، تزيد قيمته بكثير عن الحصول على آلاف كلمات السر الشخصية Passwords بسبب قدرته على فتح كثير من الأبواب المغلقة،عبر توفير معلومات دقيقة عن الثغرات المتاحة فى الشبكة المستهدفة من قبلهم.،

لا يتطلب تشغيل هذه الأداة حواسيب بمواصفات متخصصة،حيث تكفى الحواسيب الشخصية المتوفرة لدى المستخدم غير ا لمتخصص مربوطة بجهاز مودم Modeem، مع خبرة رصينة فى نظم التشغيل والشبكات، وبالخصوص برمجة المقابس Socket Programming وهى إحدى الطرق المستخدمة فى تطوير تطبيقات الزبون / الخادم Client / Server.

---

(١) المرجع ذاته – ص ٧٠ وما بعدها.

**ثانياً: الشمّام Sniffer:**

يمكن تعريف الشمام بأنه عبارة عن أى جزء من عتاد الحاسوب أو برمجياته، التى تسترق السمع وتتحسس جميع أنواع المرور المعلوماتى على الشبكة، لأغراض انتزاع أو اختطاف المعلومات المنتقلة بين أجزائها(1). يعمل الشمام على زمرة من البروتوكولات السائدة فى الشبكات الحاسوبية مثل: TCP/IP, Ethernet, IPX وغيرها من النظم حيث يباشر بوضع طرفية الشبكة Network Interface بحالة مختلطة وغير قابلة للتمييز Promiscuous Mode(*) لكى يبدأ بانتزاع جميع المعلومات المّارة خلال تلك الشبكة.

يتألف الشمّام من جزءين أحدهما من عتاد الحاسوب، والآخر من برمجياته. تعتبر بطاقة الشبكة من نوع Ethernet Card المفتاح الأساسى لعتاد الحاسوب الذى يتكئ عليه نشاط الشمام بوصفه أداة ارتباط الحاسوب بالشبكات، ومحطات العمل. أما البرمجيات فيمكن توظيف البرمجيات الشائعة فى ميدان تحليل الشبكات الحاسوبية شريطة أن تتوفر فيها خيارات متقدمة لعمليات الفحص Debugging(٢)، تكمن التهديدات المعلوماتية التى تنشب عن أنظمة الشمام فى المحاور التالية:

أ – القدرة على اقتناص كلمات العبور Passwords.

ب– القدرة على اقتناص المعلومات الخاصة، والتى تمتاز بدرجة عالية من السرية.

---

(1) Peter Grier, At War With: Sweepers, Sniffers, Trapdoors, and Worms, Air Forcce Magazine, 1997, March, pp. 20 - 24.

(*) يمكن تعريف نمط الاختلاط Promiscuous Mode بأنه عبارة عن توجيه انتباه محطات العمل Workstations صوب جميع أنشطة المرور المعلوماتى Information Traffic والإصغاء إلى ما يدور فيها، بدلاً من الاقتصار بالتعامل مع البيانات التى تخص العنوان المخصص لمجموعة العمل ذاتها.

(٢) يمكن الحصول على نسخ من الشمام على المواقع الإلكترونية التالية:

http: // mygale. mygale. org/08/datskewl/elite/

http: // hacked-inhabitants.com/warez/sunsniff.c.

جـ- إمكانية استخدامها في خرق النظم الأمنية للشبكات الحاسوبية بشتى مستوياتها.

من أجل هذا فإن وجود نظام الشمام على الشبكة المحلية يمثل تهديداً مباشراً لأمنها وأمن سريان المعلومات التي تتدفق خلالها، سواء استغل من قبل جهة خارجية (قراصنة المعلومات)، أو أحد العاملين على الشبكة ممن توجد لديهم نوايا سيئة، وأهداف تدميرية.

**ثالثاً: مصدّع كلمات العبور Passwords Cracker:**

تشمل أداة مصدع كلمات العبور، أي برنامج تطبيقي يمتلك القدرة على تجاوز عقبة شيفرة كلماتها، أو إحباط آليات الحماية المصاحبة لها.

ونود أن نلفت الانتباه في هذا المقام بأن مصدع كلمات العبور لا يلغي الشيفرة المستخدمة فيها، أو يظهرها على شكل نص مقروء Plain Text بل يتيح إمكانية تجاوز الجدار الأمني، الذي توفره لصاحبها في درء أي نشاط يسعى إلى تجاوز الحدود الشخصية لمملكة معلوماتيه الخاصة.

يتلخص عمل أدوات المصدع بمحاكاة الخوارزميات(*) الحاسوبية المستخدمة

---

(*) خوارزم Algorithm: خطوات محددة تتميز بالبساطة والوضوح لتنفيذ مهمة معينة، وفي علم البرمجة تحديد منطق تنفيذ البرنامج للوصول إلى النتيجة المرجوة منه، ويعتبر وضع الخوارزم خطوة أولية غاية في الأهمية قبل البدء في صياغة البرنامج باللغة البرمجية، ولذلك فإن الخوارزم يوضع بلغة تجريدية تسمى «لغة شبه البرمجية Psudocode»، وكانت الخوارزمات سابقاً تمثل بأشكال تسمى «أشكال التدفق flow diagrams»، ولكن صرف النظر عن هذه الطريقة لتعقيدها، على أنه توجد وسيلة جديدة لتصوير الخوارزمات تسمى أشكال «ناسي – شنايدر Ns Charts».

- تحليل الخوارزم Algorithmic analysis: تختلف الخوارزمات الممكنة لحل مسألة معنية في مدى كفاءتها، من حيث سرعة التنفيذ أو اقتصاديات المصادر المطلوبة للتنفيذ (كمساحة الذاكرة مثلاً)، لذلك وضعت قواعد رياضية ومنطقية للحكم بين الخوارزمات وانتقاء أفضلها بالنسبة لظروف التنفيذ. (مهندس/ على يوسف على – معجم مصطلحات الحاسب – مرجع سابق – ص ٢٠).

-/-

فى تشفير(*) كلمات العبور من خلال خوارزميات أعدت خصيصاً لهذا الغرض، بحيث تسعى إلى توليد شيفرات مستحدثة تناظر الشيفرات المتعمدة فى صياغة كلمة العبور الأصلية. تتألف آلية عمل نسبة كبيرة من مصدعات كلمات العبور، على مبدأ توليد حجم هائل من تعاقبات الحروف والأرقام التى تستخدم فى كلمات العبور الموظفة لدى الأفراد والمؤسسات، فتستثمر الفجوات التى تنشأ فى كلمات العبور نتيجة لاستخدام كلمات يكثر استخدامها في الحياة اليومية، أو معاجم اللغة، وصفة الكسل والتوانى لدى البعض مما ينتج عنه استخدام كلمات عبور قابلة للتصدع من خلال خوارزميات المصدع بسهولة ويسر[1].

--- - برنامج الخوارزمى: هو عبارة عن برنامج يتيح كتابة البرامج بلغة (C)، وتنقيحها ومن ثم تنفيذها. (يراجع: د/ محمد عمارة السلكة - موقع:

- www. cso. sy. net / mode / 6676.

(*) التشفير Encryption: هو منطقة تخزينية يمكن استغلالها بضراوة لتهديد الدستور والقوانين الأساسية التى تعد الملكية الفكرية منطقة مؤمنة بمقتضاه، وكذلك العدوان على حقوق الإنسان، ومثلها العدوان على حقوق المؤلف، لذا فإن التخزين الرقمى يمكن أن يوفر بيئة للمعلومات، ولكن هذه البيئة لن تكون أكثر أمناً ازاء السلبيات التى يمكن أن توفرها هذه البيئة التخزينية للقراصنة والمجرمين المعتدين على حقوق الملكية الفكرية أنظر:

- Jasonsiogfried, Christine Siedsma, Bobbie - Jo Countryman & Chester d. Hosmer, examining the Encryption Threat - Computer Forensic Research and Development center - International Journal of digital Evidence, winter 2004, Volume 2, Issue 3.

مشار إليه لدى:

د/ عمر محمد بن يونس - الإجراءات الجنائية عبر الانترنت (فى القانون الأمريكى) - دار النهضة العربية - سنة ٢٠٠٦ - ص ٢٦. ويعرف علم التشفير بأنه العلم الذى يعنى بصياغة وإنشاء زمرة متباينة من الشيفرات التى تنضوى تحت دائرة كتابة الأسرار Secret Writing. امتد أذرع هذا العلم إلى دائرة المعلوماتية وعلومها فأضحى يمثل الآليات المستخدمة لإقحام شيفرة فى البيانات أو المعلومات لضمان عدم الدخول - غير المرخص - أو إفشاء محتوياتها أثناء عمليات انتقالها بين وسائط الاتصال المعلوماتية المختلفة، بحيث تمتنع عملية اكتشاف محتوياتها أو ماهيتها إلا للأشخاص المعنيين فقط.

(1) Klien, d.V., A Survey of and Improvements to Password Security, Software engineering Instiute. Carnegie Mellon University, Pennsylvania. 1991.

**رابعاً: حصان طروادة Trojan Horse:**

يعتبر حصان طروادة من الأدوات الفاعلة في ميدان خرق الأمن المعلوماتي. وتوجد أكثر من خاصية برمجية تتصف بها النسخ المتوفرة بميدان المعلوماتية من هذه الأداة، بحيث يمكن أن نقول عنه إنه عبارة عن:

١- برنامج غير مرخص Unauthorized متضمن في برنامج شرعي Legitimate، فيباشر البرنامج غير المرخص إجراء زمرة من المهام التي لا يريدها المستخدم، أو يمتلك معلومات كافية عنها.

٢- برنامج شرعي تم تغييره بإدخال شيفرات غير مرخصة داخل هيكليته البرمجية، بحيث يقوم بجملة من الأنشطة غير المشروعة.

٣- أي برنامج يقوم بأنشطة غير مشروعة، بيد أن حشر أي شيفرة خارجية إلى هيكليته البرمجية تكسبه القدرة على القيام بأنشطة مشبوهة أو غير مشروعة.

٤- برنامج يوفر خدمة مفيدة أو مثيرة لاهتمام الآخرين، بيد أنه يقوم بأنشطة غير متوقعة، مثل سرقة كلمة العبور، أو استنساخ ملفات، أو إلغاءها دون علم المستخدم.

وقد ذهب الدكتور سولومون(١) إلى اعتباره برنامجاً يقوم بجملة فعاليات تفوق توقعات المستخدم، وتمتاز هذه الفعاليات بكونها تخريبية.

تكمن الصعوبة في تشخيص هوية برنامج حصان طروادة، في كون الأنشطة التي يقوم بها لا يمكن تمييزها عن بقية الأنشطة التقليدية السائدة في ميدان المعلوماتية، لذا لا تتوفر لدينا قرينة واضحة يمكن على أساسها إنشاء حد فاصل بين نشاط مشروع، ونشاط آخر غير مشروع بسبب استنادها جميعاً إلى دالة حاسوبية مشروعة!.

---

(1) Refer to the document found on the following addrress:
http: // www. drslomon.com/vircen/allabout.html.

إذن ليس ثمة طريق يصلح كأساس للحكم على وجود حصان طروادة، يكون عن طريق مقارنة الأنشطة، التى يقوم بها برنامج ما مع قائمة الأنشطة التى يتوقعها المستخدم لذلك البرنامج، وهذا أمر يعصب مناله؟

يتم صناعة خيول طروادة بواسطة فئة معينة من المبرمجين الماهرين، لذا فإن وصول أى من ملفات هذا النوع لا يتم إلا عن طريق استلام ملف يحوى على هذه الآفة - عبر أى قناة من قنوات تداول الملفات الحاسوبية - قد تم إعداده بواسطة مبرمج متخصص، وليس ثمة احتمال نشوء حصان طروادة نتيجة لعملية طباعة عشوائية يقوم بها مستخدم ما - كما يتوهم البعض - على الحاسوب حتى لو استمرت هذه العملية بضعة أيام.

تتم صياغة الهيكلية البرمجية لحصان طروادة من قبل المبرمج لتحقيق غايات، وأهداف محددة يمكن حصرها فى دائرة الأمن المعلوماتى بالمحاور التالية:

١- القيام بجملة من الأنشطة المعلوماتية التى توفر لصانعه معلومات مفيدة وحيوية حول النظام المستهدف بهذه الأداة، أو التعرض والتشهير بالنظام من خلال كشف أسراره.

٢- إخفاء بعض الدول المتاحة فى النظام، والتى يعتبرها صاحب البرنامج ذات أهمية خاصة فى ذلك النظام.

٣- إحداث خلل فى النظام المعلوماتى المستخدم مثل: إلغاء الملفات، وتغيير مقومات النظام، أو إيقافه كلياً عن العمل... الخ.

قد تقوم بعض أنواع خيول طروادة بهذه الأنشطة مجتمعة، أو يختص بعضها بنشاط دون آخر. ويمكن وراء هذه الأنشطة اتصاف هذه الأداة بالقدرة على الأداء الذكى لجملة من المهام المعلوماتية، التى تتميز بقدرتها على اختراق الحواجز الأمنية التى يقيمها النظام المعلوماتى، مع إمكانية الجمع

بين أكثر من خاصية تدميرية فى آن واحد، ومهام أخرى تستبطن أهدافاً تخريبية بالنظام المستهدف.

إن شريحة المبرمجين التى تقوم باعداد خيول طروادة تنقسم إلى فئتين:

**(الفئة الأولي)**، وهم مبرمجون شباب، يتوهمون أن فى هذا العمل التخريبى إثباتاً لقدراتهم البرمجية. فلا تحمل خيولهم أهدافاً استراتيجية بعيدة المدى، وتتصف بقدرة تخريبية سطحية لا تمثل لإدارة نظام الشبكات قلقاً كبيراً.

**(الفئة الثانية)**، وتتألف من زمرة من المتخصصين الذين يعملون فى إدارة نظم الشبكات الحاسوبية، ويمتلكون خبرة عميقة فى هذا المضمار الحيوى، فيباشرون مثل هذا النشاط التخريبى لتحقيق غايات مبيتة تميل باتجاه جلب منفعة شخصية أو منفعة للغير، عن طريق كشف أسرار الأنشطة المعلوماتية السائدة فى شبكة ما، بمختلف مستوياتها، أو إنشاء ثغرة تمكن من الدخول إلى أكثر أعماقها بعداً، حيث الأسرار التى لا تقدر بثمن؟ ولا يمكن الكشف عن هذه النوع إلا عن طريق المصادفة البحتة بظهور خلل معين فى أداء النظام، يعكس وجود مثل هذا النوع من خيول طروادة.

إن وجود مثل هذه الأنشطة فى شبكات محلية، أو متخصصة يجعل عدداً كبيراً من الحواسيب المرتبطة بتلك الشبكة عرضة للهجمات المعلوماتية، وعاجزة عن غلق الأبواب على أسرارها أمام الاستهداف الاستخبارى لخيول طروادة!.

ويكمن التهديد المعلوماتى الذى يحمله حصان طروادة إلى النظام المصاب، فى صعوبة تحديد مستوى الاختراق الذى حققته هذه الأداة فى النظام، الأمر الذى يورث لإدارة النظام قلقاً مستمراً، حتى بعد اكتشافه لصعوبة تحديد حجم الاختراق، والمدى الذى ستمتد إليه تأثيراته.

من أجل هذا إن لم تكن إدارة نظام الشبكات الرئيسة للمعلومات تمتلك معلومات رصينة، وعميقة فى ميدان الأمن المعلوماتى، فإن خيول طروادة

سوف تمتلك فرصة جديدة لهتك أسرار قواعد المعلومات الاستراتيجية، قبل عدة أشهر من توفر فرصة مواتية لاكتشافها.

**خامساً: قنبلة البريد الإلكتروني E-mail Bomb:**

تتمثل قنبلة البريد الإلكترونى ببرنامج حاسوبى يعمد إلى القصف المستمر للعنوان المستهدف Target Address عن طريق إرسال حزمة من رسائل البريد الإلكترونى فى توقيت محدد، وبعدد معين، وخلال بعد زمنى يتم اختياره من قبل الشخص الذى يباشر عملية الاستهداف.

ينشب عن نشاط قنبلة البريد الإلكترونى إزعاج دائم للجهة المستهدفة نتيجة للتدفق الهائل لرسائل البريد الإلكترونى، دون إحداث اضرار أخرى، ويمكن التغلب على هذه الأداة عبر استخدام نظام استبعاد Exclusionary Scheme بعد تحديد مصدر التهديد المعلوماتى، عن طريق استثمار القابليات المتاحة فى المستعرضات الشائعة على الشبكة مثل Netscape Navigator والتى تساعد على إظهار مصدر الخادم البريدى Mail Server، الذى تأتى منه حزمة البريد الإلكترونى غير المنقطعة. ثم تبدأ عملية معالجة الموقف لكفّ عملية الاستهداف اللامشروع.

**سادساً: الفيروس بوصفة تهديد لأمن المعلوماتية:**

يصعب على المستخدم العادى والمتخصص تحديد الفترة الزمنية التى ظهرت فيها فيروسات الحاسوب، وازدياد أعدادها بشكل ملحوظ، بحيث أصبحت البرمجيات الخاصة بالكشف عن وجودها أو معالجتها جزءاً لا يتجزأ من جعبة أدوات المستخدم الأساسية(*).

---

(*) واختراق شبكة المعلومات قد يكون هدفه زرع فيروس فى النظام المعلوماتى من أجل تدميره، كما أن الجانى قد يهدف من ذلك إلى سرقة هذه المعلومات بوصفها مالاً، وبوصفها من الكيانات الاقتصادية المستحدثة. سيما وأن المعلومات التى تستهدف قد تكون من المعلومات المالية أو المعلومات التجارية والصناعية والمعلومات العسكرية، وكذلك المعلومات الشخصية. د/ رياض سليمان عواد، أمن المعلومات وضرورة وضع تشريع لجرائم الحاسب الآلى، مجلة الدراسات والثقافة الشرطية، وزارة الداخلية بدولة الأمارات، العدد ٣٥٩ السنة ٢٠ نوفمبر ٢٠٠٠، ص ٤٦ وما بعدها.

ظهرت مجموعة متباينة من التعاريف الاصطلاحية للفيروس، وهى تحاول أن توفر له تعريفاً، جامعاً، مانعاً، يضم بين ثنايا مفرداتها الاصطلاحية معظم الخصائص السلوكية التى يتصف بها[١]: فعرفه البعض[٢] بأنه عبارة عن فئة محددة من البرمجيات التى تمتاز بتأثيرها التخريبى على نظم تشغيل الحاسوب وبرمجياته، وتحتوى على برنامج من نوع الديدان تصحبة قنبلة موقوتة زمنياً أو منطقياً، أو جزء محدد من برميجات خيول طروادة.

وذهب البعض الآخر[٣] إلى تعريفه بأنه برنامج صغير يلتصق ببرمجيات أخرى تساعده على عمليات الاختفاء، فتمهد بذلك الطريق أمام انتقاله بين نظم التشغيل بسهولة، لكى يباشر بعمله التخريبى الذى يشمل عملية تكوين نسخ متعددة فى الحاسوب المصاب.

بالمقابل عرفته باتريشيا هوفمان[٤] بأنه البرنامج الذى يقوم بتغيير محتوى البرمجيات التى يصيبها عن طريق إلصاق نسخة منه فيها، بينما أضفى عليه توم مينالى[٥] شمولية أكبر باعتباره مجموعة ايعازات برمجية قد صممت من قبل شخص ما، للتسلل إلى حاسوب محايد، بغرض إجراء جملة من الفعاليات التى قد تشمل: تكوين نسخ إضافية تلتصق بالبرمجيات الأخرى، أو تصدر رسائل مزعجة، أو ينجم عنها تأثيرات ضارة كإلغاء الملفات أو إحداث خلل فى هيكليتها.

أما تعريف أحد الأقطاب الرئيسة لبرمجيات الحاسوب الشخصى بيتر نورتون، صانع سلسلة برمجيات صيانة الحاسوب ومكافحة الفيروسات الشهيرة

---

(١) أ/ حسن مظفر الرزو – المرجع السابق –ص ٧٧ وما بعدها.

(2) Hard Disk Survival, p. 213.

(3) Computer Viruses, p. 3.

(4) F-Prot, User Manual, Version 2.26, 1993.

(5) Windows Computing, June, 1997, p. 27.

فقد ذهب إلى تعريفه[1] بأنه عبارة عن برنامج صغير قد صيغ لغرض تغيير عمل برمجيات الحاسوب، دون السماح للمستخدم بمعرفة هذا الأمر.

**ويلاحظ أن هناك خاصيتان أساسيتان يفتقر إليهما الفيروس:**

**الأولى:** القدرة على التشغيل الذاتي عن طريق إدارج شيفرته في المسار التشغيلي لبرنامج آخر.

**والثانية:** ضرورة إنشائه نسخاً إضافية تزيد من مساحة انتشاره.

لقد تفاقمت مشكلة انتشار الفيروسات في ميدان الحاسوب، وتعددت أنواعها باختلاف هيكلية البرمجة، ومواطن استقرارها، وطبيعة التأثيرات الناجمة عنها، ونوع الملفات التي تستهدفها في تأثيراتها، بحيث لم يعد من السهل التعامل معها ما لم تصنف إلى أصناف محددة، يجمعها قاسم مشترك واحد، لكي يسهل تحديد هويتها، وطرائق معالجتها(*).

(1) Norton Anti Virus User's Manual, Version 4.0, 1998.

(*) لعل قصة (موريس) مصمم فيروس (الدودة) – ويسمى فيروس (موريس)، خير دليل على مدى تفاقم مشكلة انتشار الفيروسات في مجال نظم المعلومات، وكونها من أهم وسائل اختراق الأمن المعلوماتي.

وصاحب هذا الفيروس هو الطالب الأمريكي (روبرت موريس) يدرس في جامعة كورنل، وقد اكتسب خبرة عظيمة في علوم الكمبيوتر، أثناء دراسته بجامعة (هارفارد)، واستخدم الإنترنت لتطوير برنامج للكومبيوتر عرف فيما بعد باسم الدودة Worm أو فيروس الإنترنت، وكان هدف الطالب من تطوير هذا البرنامج أن يثبت عدم قدرة الاجراءات الأمنية القائمة لحماية شبكات الكومبيوتر، وذلك باظهار العيوب التي اكتشفها.

– وقد قام بتصميم البرنامج بحيث ينتشر بشبكة وطنية للكومبيوتر بعد أن يتم تشغيله عن طريق حاسب آلي محلي مرتبط بهذه الشبكة، وقام موريس بتشغيل البرنامج على الإنترنت، والذي يربط بين مجموعة من شبكات الكومبيوتر الأمريكية التي تربط بدورها بين أجهزة كمبيوتر خاصة بالجامعات والجهات الإدارية الحكومية وجهات عسكرية.

– وكانت خطة موريس أن ينتشر الفيروس دون جذب الانتباه إليه، سيما وأنه توقع أن يعمل لفترة قصيرة من الوقت دون أن يشعر به المبرمجون أو قبل أن يمكنهم القضاء عليه، كذلك روعي في تصميم الفيروس ألا ينسخ نفسه على حاسب آلي سبق أن نسخ عليه حتى لا يتم اكتشافه، وتوقع أن يتم القضاء عليه بمجرد ايقاف الحاسب المصاب.

– ولكن الذي حدث أن الفيروس انتشر بسرعة كبيرة، وأدى إلى توقف الكثير من أجهزة

في بدايات عملية التصنيف، تم تقسم الفيروسات إلي قسمين أساسيين هما:

أ - فيروسات قاطع التحميل Boot Sector Virus BSV:

وينضوى تحت لوائها الفيروسات التى تمتلك القدرة على إصابة قاطع التحميل فى وسائط الخزن Boot Sector، حيث تستبدل القطاع الرئيس بآخر من

---

— الحاسب الآلى فى الولايات المتحدة عن العمل أو جعلها تعمل بصورة غير سليمة، وحاول الطالب المذكور ايقاف الڤيروس بمعاونة صديق له دون جدوى، حيث إتفقا على ارسال رسائل لا تحمل اسمه إلى مبرمجي الكومبيوتر بأنحاء الولايات المتحدة لاخطارهم بطريقة القضاء على الڤيروس، ولم يتمكنا من ارسال هذه الرسائل، لأن أجهزة الحاسب الآلى فى أنحاء البلاد قد أصيبت.

– وترتب على نشاط الطالب المذكور توقف أجهزة حاسب آلى حيوية عن العمل فى الجامعات والمراكز البحثية والمواقع العسكرية، وتراوحت تكاليف الاصلاح ما بين (٢٠٠) دولار إلى (٥٣,٠٠٠) دولار أمريكى لكل جهة على حدة.

– وكان سبب إنتشار الڤيروس هو استغلال ثغرة فى نمط ازالة الشوائب الخاصة ببرنامج البريد الإليكترونى عبر نظام يسمى يونكس (Unix) وهو نمط يعمل على جهاز حاسوبي موصول عبر الشبكة، بانتظار أن ينتقل إلى جهاز آخر لتسليم البريد الإليكترونى، وتقع الثغرة فى فترة الانتظار المذكورة.

– وقد قام فريق من جامعتى Berkeley و Mit بالعمل على تفكيك الڤيروس وتحييده، وذلك عن طريق اعادته إلى مصدره الأول لمعرفة طريقة عمله، وتوصلوا فى النهاية إلى طريقة لوقف انتشار الڤيروس.

– وقد حوكم الطالب بمقتضى قانون ڤيدرالى أمريكى يجرم الدخول إلى أجهزة الحاسب الآلى عمداً ودون تصريح، وبأى وسيلة تؤدى إلى تدمير أو تخريب المعلومات الموجودة عليه، ودافع عن نفسه بانتفاء نية الضرر لديه، لكن المحكمة رأت أنه لا يشترط اتجاه النية إلى تحقيق الضرر، بل يكفى أن تتجه نية الجانى إلى الدخول غير المشروع على نظام الحاسب الآلى الڤيدرالى. وقد حكم ضده بالوضع ثلاث سنوات تحت المراقبة، والقيام بعمل لمدة ٤٠٠ ساعة فى خدمة المجتمع، وغرامة مقدارها ١٠,٠٥٠ آلاف دولار أمريكى بالإضافة إلى تكاليف وضعه تحت المراقبة، وقد تأيد هذا الحكم استئنافياً.

* يراجع فيما سبق:

د/ عبادة أحمد عبادة، التدمير المتعمد لأنظمة المعلومات الإليكترونية، بحث لدى مركز البحوث والدراسات – شرطة امارة دبى – الامارات العربية المتحدة – العدد (٨٧)، مارس ١٩٩٩، وكذلك د/ مدحت رمضان، جرائم الاعتداء على الأشخاص والإنترنت، دار النهضة العربية، القاهرة، عام ٢٠٠٠، ص ١٢ وما بعدها.

صنع الفيروس مع إمكانية تكوين نسخة إضافية منه، لإيهام المستخدم بعدم وجود فيروس فى حاسوبه الشخصى.

**ب - الفيروسات البرمجية Program Viruses:**

وتضم بين جنباتها الفيروسات التى تلتصق بالبرمجيات التطبيقية - التشغيلية، والتى تمتلك امتداداً من نوع (*.dll. *.com. ".exe.*) .

بقى هذا التصنيف سائداً فى ميدان فيروسات الحاسوب، لحين ظهور أنواع جديدة استخدام صانعوها تقنيات متقدمة، لصياغة هيكليتها وإحكام بنيتها بحيث لم يعد هذا التصنيف كافياً لوصفها، فظهرت تصانيف جديدة أكثر تفصيلاً ولعل أهم محاور التصنيف فى الوقت الحالى هى[1]:

- **الصنف الأول:** فيروسات عدوى قاطع التحميل وجدول القاطعBoot Sector .
- **الصنف الثاني:** فيروسات عدوى النظام System Infector .
- **الصنف الثالث:** فيروسات عدوى البرمجيات التطبيقية Generic Application Infector .
- **الصنف الرابع:** الفيروسات معددة التراكيب Polymorphic Viruses .
- **الصنف الخامس:** فيروسات الماكرو Macro Viruses .

**سابعاً: مخاطر تهدد نظم المعلومات[2]:**

تأخذ المخاطر التى قد تتعرض لها نظم المعلومات عدة أشكال. يتمثل أهمها فيما يلى:

**١- التهديد بالتغيير:**

يعتبر هذا العمل من أخطر الأعمال غير المشروعة ضد مستخدمى شبكة

---

(١) أ/ حسن مظفر الوزو - مرجع سابق - ص ٧٨ .

(٢) د/ عبد الكريم أبو الفتوح درويش - تأمين نظم المعلومات - مجلة الأمن العام - القاهرة، العدد ١٧٣ - ابريل ٢٠٠١ .

نظم المعلومات (الانترنت) فعلى سبيل المثال. يمكن للقائم بالعمل غير المشروع (مهاجم النظام) تعديل برنامج تصفح الانترنت (Web Browser) أو أى برنامج آخر يتم تشغيله. وبذلك يمكن للمجرم هنا أن يتحكم فى الكمبيوتر من قبل الغير. وفى معظم أنواع النظم. يعطى هذا الفعل المجرم القدرة على قراءة. وتعديل. ومسح أى ملف، أو إرساله بالبريد الالكترونى إلى أى مكان على الانترنت (وذلك فى حالة اتصال نظام المعلومات بالانترنت)، أو القيام بأى فعل آخر يمكن للمستخدم الأصلى للنظام القيام به. ومن الأفعال غير المشروعة الأخرى التى قد يقوم بها الشخص القائم بالدخول على النظام، استخدام أو تغيير بيانات الخادم (Server) وتعديل الذاكرة. وتعديل البيانات أثناء إرسالها(١).

٢- التهديد بكشف سرية المعلومات:

قد يتمثل هدف القائم بالفعل غير المشروع فى إفشاء سرية المعلومات، الخاصة بأجهزة الكمبيوتر الداخلة فى تكوين نظام المعلومات. مثل البيانات التى تصف إمكانات ونوعية الكمبيوتر. والأماكن التى يتصل بها وعناوينها(٢).

٣- استخدام العناوين بطرق غير مشروعة:

قد يقوم القائم بالفعل غير المشروع بإعداد عناوين مماثلة لبروتوكولات الانترنت المملوكة لبعض الجهات أو الأفراد، وبالتالى استخدامها بطرق غير مشروعة تحت غطاء أسماء غير أسمائهم، والتى عندما يريد شخص الاتصال بالجهة، أو الفرد الأصلى مالك العنوان. أو العناوين. فإنه يتصل بجهة الفرد القائم بالعمل غير المشروع بدلا من الشخص الأصلى(٣).

(1) Aviel d. Rubin, Danied Geer and Marcus, J. Ranam, Web Secanity Searce Book A Complete Guideto wels Sčuri Threats and Sqlations and Servers Write Secare Java Applets and Cgi Scripts Avoid Security Holesn Populor Browcers, Witey ? Compiter Publishing Johin Wotey and Sons, Jns, New York, 1997, Page, 12, 13.

(2) Ibid., P. 15.

(3) Ibid., Pp. 15 - 16.

٤- خدعة العملاء المتعاملين مع جهات محددة:

قد يلجأ القائم بالفعل غير المشروع إلى حيلة أخرى لايقاع طالبى التعامل مع جهات محددة فى فخ التعامل مع غيرها من الجهات. وهنا يلجأ القائم بالعمل غير المشروع بخداع العملاء عن طريق إنشاء عنوان بريدى مشابهة فى تكوينه للعنوان البريدى لجهة ما يقوم العديد من العملاء بالتعامل معها. وهذا قد يستخدم مقطع من عنوان بريذى بصورة مشابهة لعنوان بريدى لجهة أخرى مثل أستخدام VBN Com بدلا من VBM CON، لأنه في كثير من الأحوال عندما يحاول الأفراد كتابة العنوان الصحيح قد يخطئون فى الهجاء. فيكتب حرف N بدلا من حرف M (حيث إنه الحرف المجاور له على لوحة مفاتيح الكتابة بالنسبة للكمبيوتر). وهنا يدخل الفرد على موقع آخر غير الموقع الذى يريد الدخول عليه أصلاً. وبالتالى قد يساء أستخدام البيانات والمعلومات التى ترسل إلى هذا الموقع. مثل كلمات المرور. وأرقام كروت الدفع الإلكترونى. وخاصة ما هو غير مشفر منها(١).

٥- منع تقديم الخدمة أو إبطائها:

يعد من أخطر الأفعال غير المشروعة ضد نظم المعلومات، استخدام أساليب عديدة لمنع تقديم الخدمة، أو على الأقل إبطائها مثل الدخول على موقع أى جهة على الإنترنت(Internet Sile)، وطلب كم هائل من الخدمات فى وقت واحد من خلال الخادم الخاص بها. وبالتالى يتم إشغال هذا الخادم عن محاولة البدء فى إجراءات تقديم الخدمة. أو رفض تقديمها من خلال فحص المعلومات المقدمة له. وهو الأمر الذى يترتب عليه عدم اتاحة الوقت اللازم لتقديم الخدمة للعملاء الشرعيين. أو على الأقل إبطاء سرعة تقدنيم الخدمة بصورة كبيرة بما يؤثر على رضاء المشتركين فى الخدمة عن مدى كفاءة تقديمها لهم(٢).

(1) Ibid Pp. 15 - 16.

(2) Ibid., pp. 15 - 16.

## المطلب الثاني

## تطبيقات عملية لاختراق

## نظم أمن المعلوماتية

### أولاً: فيروس البريد الإلكتروني:

من أمثلة الفيروسات التى تصيب البرمجيات، نستعرض قضية المتهم المعلوماتى ديفيد سميث مع فيروس – ميليسيا – وهو فيروس البريد الإلكترونى الأكثر شهرة، حيث اعتقلت الشرطة في ولاية – نيوجرسى – بالولايات المتحدة الأمريكية المتهم المذكور، والذى أنشأ ڤيروس البريد الإليكترونى الذى عرف باسم – ميليسيا – وأحدث اضطراباً عالمياً فى البريد الإليكترونى بشبكة الإنترنت، وقد قُضى ضده بالسجن لعقوبات تصل إلى (٤٠) عاماً، وغرامة نقدية قيمتها (٤٨٠) ألف دولار[1].

---

(١) راجع فى ذلك د/ جميل عبد الباقى – مرجع سابق – ص ٤٩ وما بعدها.

- وتخلص قصة ڤيروس – ميليسا – فى أنه فى ١٩٩٩/٣/٢٦ أصيبت الآلاف من أجهزة الحاسب الآلى بفيروس اثقل كاهل عمل – البريد الإليكترونى – فى مختلفت انحاء العالم – وهذا الڤيروس يستنسخ نفسه، ويسخر برمجيات البريد الإليكترونى لارسال قائمة بعناوين المواقع الجنسية الفاضحة ونشرها بسرعة من خلال الإنترنت، الأمر الذى أجبر العديد من الشركات على اغلاق مزودات خدمة البريد الإليكترونى لديها.
- وعطل الڤيروس العديد من مزودات خدمة البريد الإليكترونى التابعة لشركات الكومبيوتر العملاقة – إنتل، ومايكروسوفت، وكذلك لدى وزارة الدفاع الأمريكية، ووصف بأنه الفيروس الأكثر إنتشاراً على الإطلاق فى تاريخ الكومبيوتر، وكثرت الشائعات حوله، وساهم المتحدث باسم – البنتاجون – بزيادة هذه الشائعات حين أعلن خشيته من أن يكون العرب وراء الڤيروس، وذلك لتزامن انتشار هذا الڤيروس مع هجوم الولايات المتحدة، وحلف شمال الأطلنطى على الصرب فى جمهورية يوغسلافيا السابقة.
- وهذا الڤيروس يرسل قائمة بعناوين (٨٠) موقعاً جنسياً إلى (٥٠) شخص فى سجل عناوين المجنى عليهم – أصحاب البريد الإليكترونى – فلو أصيب جهاز واحد بهذا الڤيروس فإنه يعمد إلى إرسال خمسين رسالة إلى خمسين جهة مسجلة فى العنوان الواحد الذى أصابه، وهذا هو السبب الذى جعل أغلب المصابين بالڤيروس من الذين تبدأ أسماؤهم بحرف -A- , -B- وقد سارعت الشركات المتخصصة مثل – ماك أفى سكان – ، بى – سى – سيللين، إلى اصدار

=/=

المضادات اللازمة لوقف انتشار الفيروس خلال ساعات، ولكن هذه الساعات كانت كفيلة بانتشار الفيروس على نحو وبائى، وبذلت يومى ٢٧، ٢٨ مارس ١٩٩٩ جهوداً كبيرة لإصلاح أثار هذا الفيروس المدمرة، وتصميم البرامج المضادة له، وبدءاً من يوم الأحد ١٩٩٩/٣/٢٩ بدأ البحث عن المجرم صاحب هذا الفيروس.

– وكانت الرسالة الملوثة بالفيروس والتى ترسل بالبريد الإليكترونى إلى المشترك تحمل عبارة باسم صاحب الجهاز هى Message from usermame Jsemame وذلك عقب رسالة Improtant subject حتى يسارع صاحب البريد الإليكترونى بفتح الرسالة، والتى كانت تضمن عبارات مشوقة مثل Here is that: document you asked for don't show any one وبمجرد أن يفتح أحد المتلقين الرسالة والنص المربوط بها، يرسل الفيروس مرة أخرى إلى خمسين شخصاً أخرين، وهذا هو السبب الذى جعل الفيروس ينتشر فى نظم البريد الإليكترونى خلال ساعات محدودة منذ إطلاقه، جدير بالذكر كذلك أن هذا الفيروس كان يعمل بصفة متكاملة حسب برنامج – أوتلوك – لكن فى برامج أخرى مثل لوتس نوتس. توفيل جروب وليز، نتسكيب ماستجر – فإن الفيروس لم يكن ينتشر بصفة تلقائية، إنما كان يلوث البرامج بالجهاز الذى أرسل إليه وكذلك ملفات – Word – فى ذات الجهاز إن أعيد فتحه مرة أخرى.

– وبدأ رجال المباحث الفيدرالية الأمريكية، البحث عن مبتكر هذا الفيروس، لكن الكثير منهم كان يشك فى وجود مجرم واقعى أو حقيقى، وقد انتهى البحث إلى أن المشتبه فيه شخص يدعى "Sky Rocket" وتنطلق أعماله من شبكة – أمريكا أون لاين – وموقعها على الإنترنت http: // www. aol. com، وهذا الاسم محرف عن صاروخ الفضاء، وهو اسم تجارى شائع لبعض التجهيزات والألعاب علاوة على استخدامه، ككناية عن سرعة الانطلاق والتحليق بسرعة.

– لكن شركة Network Associates inc. المتخصصة فى أنظمة أمان الكومبيوتر، توصلت إلى وجود علاقة بين فيروس ميليسا وسكاى روكت، وبين فيروسات أخرى ظهرت قبله خلال عام، حيث تأكد أن Sky Roket اسم لأحد مستخدمى موقع – أمريكا أون لاين – وقد تم السطو عليه من قبل الهاكرز، الذين يسرقوا كلمات السر، للحصول على الخدمات مجاناً أو لتغطية بعض نشاطاتهم غير المشروعة على الشبكة.

– وأكد جهاز التحقيق، أن المالك الحقيقى لعنوان – سكاى روكت – برئ من هذه التهمة، وأن الذى ينتحل شخصيته هو المبتكر الحقيقى لهذا الفيروس، وتم – التتبع العكسى لأثر سكاى روكت – على شبكة الإنترنت، وتبين أن الفيروس انطلق لأول مرة من الترويج ضمن منتدى كان يناقش موضوعات أباحية، وحرصت الشرطة الفيدرالية على أحاطة عملها بسرية تامة، وساعدتها شبكة أمريكا أون لاين، وبدأت تضييق الخناق على الجانى – الذى وشى به أحد الأشخاص، وبدأت خطوات ملاحقته سريعاً حيث ألقى القبض على الجانى مساء الخميس الأول من أبريل، وتبين أنه شخص يدعى – ديفيد سميث – فى الثلاثين من عمره، ووجهت

-/-

-- له السلطات تهمة تخريب أنظمة الاتصالات العامة والتآمر والسطو على خدمات الكومبيوتر وهى اتهامات تصل عقوبتها إلى السجن مدة (٤٠) عاماً، وغرامة نقدية تصل قيمتها إلى (٤٨٠) ألف دولار.

- وقد حاول محاميه تعبئة الرأى العام للدفاع عنه بوصفه مريض نفقسياً حيث قال: «إن عالم الكومبيوتر ملئ بالبشر الذين يقومون بتجارب واختبارات، وأن موكله لم يفعل شيئاً عن سوء نية، ولم يكن يقصد القيام بشئ من هذا القبيل، إنه يبدو اليوم مضطرباً ومذعوراً ومعكر المزاج، إنه يعانى من محنة حقيقية» - راجع فى قصة ڤيروس ميليسا كاملة د/ ممدوح عبد الحميد عبد المطلب - جرائم استخدام الكومبيوتر وشبكة المعلومات العالمية - مرجع سابق، ص ص ١٦٩ - ١٧٤. وكذلك د/ جميل عبد الباقى، المرجع السابق، ص ٤٩.

- ويذكر أنه بتاريخ ١٩٩٩/١١/١٠ ظهر نوع من الڤيروسات يضرب البريد الإليكترونى شبيه بڤيروس ميليسا، وذلك بعد القبض على ديڤيد سميث مخترع الڤيروس المذكور.

- وجاء فى الخبر عن هذا الڤيروس أنه يظهر فى صورة رسالة فى صندوق البريد الإليكترونى فى جهاز كمبيوتر واحد، ثم يبدأ بعد ذلك فى احداث فوضى واسعة بين أعداد كبيرة جداً من أجهزة الكومبيوتر، وقد سمى هذا الڤيروس - بابل بوى - ووصل بالفعل لعدد من الباحثين فى شركة نيتوورك أسوشيتس - المتخصصة فى نظم تأمين أجهزة الكومبيوتر وتطبيقاته.

- وقال خبراء الكومبيوتر أن ظهور هذا الڤيروس يعد ميلاداً لجيل جديد من ڤيروسات الكومبيوتر، لأنه قضى على الاعتقاد الذى كان سائداً لفترة طويلة من أنه لا يمكن لأى ڤيروس أن ينتقل إلى جهاز كمبيوتر عن طريق البريد الإليكترونى إلا إذا فتح مستخدمه أحد الملفات التى تحمل الڤيروس والملحقة برسالة عبر البريد الإليكترونى، وقد وجدت الشركات المعنية أن تهديد هذا البيروس خطير لدرجة تنبئ بهجمة شرسة لأنواع جديدة من الڤيروسات، ومشكلة هذا الڤيروس أنه لا يدمر الأجهزة فقط وإنما يعمل بشكل مشابه لڤيروس ميليسا الشهير، حيث يرسل نفسه إلى جميع العناوين الموجودة على قائمة البريد الإليكترونى لجهاز الحاسب الآلى المصاب.

- وذكر مدير إحدى شركات مكافحة ڤيروس الكومبيوتر، أنه إذا لم يكن لدى مستخدمى الكومبيوتر برامج مكافحة ڤيروسات الكومبيوتر المستحدثة، فإن ذلك سوف يعنى استحالة ايقاف ڤيروس - بابل بوى - لأن مجرد ارسال هذا الڤيروس إلى أى جهاز، يعنى اصابة الجهاز بالفعل، لذلك فقد عكفت شركات مكافحة فيروس الكومبيوتر على اضافة أدوات لوقف هذا الڤيروس إلى مواقعها على الإنترنت حتى تحيط بها العملاء - لمزيد من التفصيلات حول هذا الڤيروس - راجع مقالة بعنوان ڤيروس من عائلة ميليسا يهدد شبكات الكومبيوتر - بتاريخ ١٩٩٩/١١/١٠ على موقع http:// news. bbc. co.uk/arabic/news.newswsid.

- والحقيقة أن الڤيروسات التى تنطلق إلى البريد الإليكترونى وتؤثر فيه، تجعل من القول بسلامة تناول الرسائل والبيانات عن طريق هذا البريد، قول غير مطلق وغير صحيح بشكل تام، فضلاً عن أنه يضيف خبرات ضارة من ذلك البريد الإليكترونى الذى يحتفظ بموقع أو أكثر فيه، وهو مدخل لاصابة الجهاز الذى يستخدم بڤيروس من هذه الڤيروسات.

**ثانياً: الثغرات المعلوماتية Holes[1]:**

تعد الثغرات المعلوماتية باباً شرعياً أمام الهجمات وأنواع الاختراقات التى تسود فى دائرة النظم المعلوماتية بشتى مستوياتها، لكونها تمثل المناطق التى يستغلها الآخر فى التسلل إلى النظم المعلوماتية تمهيداً لمباشرة عمليات تخريبية.

إن الثغرة المعلوماتية هى عبارة عن هيئة أو خاصية تقنية يتصف بها عتاد الحاسوب أو برمجياته التطبيقية والتى تتيح للمستخدم غير المرخص Unauthorized User إمكانية اقتناص فرصة الدخول إلى النظام المعلوماتى، أو زيادة مستوى الدخول إلى حدود غير متاحة له بدون وجود هذه الثغرة.

تشمل الثغرة المعلوماتية مساحة واسعة فى ميدان التقنيات المعلوماتية، فيندرج بدائرتها أى جزء فى العتاد Computer Hardware أو البرمجيات Software توفر للغير إمكانية الدخول، أو اختراق الحواجز المعلوماتية – الأمنية، ولتوضيح هذا الأمر سنذكر مثالين:

**المثال الأول:** تعتبر عملية إلغاء محتويات كلمة العبور الموجودة فى CMOS اللوح الأم بالحاسوب عند رفع بطاريته، ثغرة معلوماتية تمكن الغير من تجاوز عقبة كلمة المرور والدخول إلى ساحة الحاسوب الشخصى بدون ترخيص!.

**المثال الثاني:** إن اعتماد مبدأ التشغيل للمستخدم المنفرد Single-User Mode فى نظم محطات الشبكات الحاسوبية، يمكن اعتباره ثغرة معلوماتية لتوفيره الفرصة لمستخدم ما – يحمل نوايا – سيئة بإدخال إيعازات برمجية تتيح له إمكانية إحكام السيطرة على أنشطة مختلفة تسود النظام.

بعبارة أخرى ليس ثمة موقع على ساحة المعلوماتية يمتلك أمناً مطلقاً، لاحتمال وجود أكثر من ثغرة غير منظورة، تتيحها الخصائص التقنية لعتاد الحاسوب أو تقنياته، فتكون عرضة للاختراق.

---

(١) أ/ حسن مظفر الرزو – مرجع سابق – ص ص ٨٠ ، ٨١.

وتتبـاين خطورة الأضرار الناجمة عن استغلال(بأختلاف أنواعـها) هذه الثغرات، وطبيعة الهجمة المعلوماتية التى تتسلل من خلالها، فتتراوح بين إحداث أنشطة مزعجة لإدارة النظام ومستخدميه، وتتفاقم باتجاه التدمير الشامل للنظام بكافة مكوناته.

يظهـر فى جـدول رقم (١) أنواع الثـغرات المعلومـاتيـة السـائدة فى النظام المعلوماتى، ومعامل الخطورة الناشية عن كل منها.

جدول رقم (١): أنواع الثغرات المعلوماتية وطبيعة المخاطر الناشئة عنها

| التصنيف | طبيعة الثغرة والمخاطر المصاحبة لها |
|---|---|
| A | ثغرة توفر لغير مستخدمى النظام، إمكانية التدمير الشامل للنظام المعلوماتى، عن طريق إتاحة الفرصة لجهات خارجة عن النظام الدخول إليه (عبر مضيف بعيد) وممارسة أنشطة تدميرية ببنية النظام. |
| B | ثغرة توفر لمستخدمى النظام إمكانية زيادة مستوى الترخيص، فى استخدام مواقع محظورة بالنظام، وإحكام السيطرة على أنشطة محددة بالنظام. |
| C | ثغرة توفر لمستخدم ما، داخل النظام المعلوماتى أو خارجه، إمكانية إحباط، أو مقاطعة،أو معارضة أنشطة سائدة على النظام المعلوماتى. |

**ثالثاً: قرصان المعلومات Hacker(*):**

أثمر البحث فى ميدان المعاجم اللغوية عن الأصول المعجمية لهذه الكلمة –

(*) ظهر أكثر من تعريف لاصطلاحى قراصنة المعلومات ومصدعى كلمات العبور Hackers & Carckers بعضـها انتشرت فى أوساط العامة، وامتـازت بعدم وضوح الفرق القائم بين

–/–

التى أستُعيرت من ميدان اللغة إلى ساحة الاصطلاحات المعلوماتية - عن تحديد أهم المعانى التى تكمن وراءها. يستخدم فعل Hack لإشارة إلى: مباشرة عملية التقطيع لشئ ما، الأمر الذى يشير إلى طبيعة النشاط الذى يمارسة قرصان المعلومات(١).

من أجل هذا فقد عُرِّف قرصان المعلومات Hacker بأنه شخص يمتلك خبرة عميقة فى ميدان تقنيات المعلوماتية(٢)، له القدرة على استغلال معرفته للولوج فى الأعماق المظلمة، والمحظورة من نظم شبكات الحواسيب، بشتى مستوياتها.

وتهدف عملية دخوله اللامشروع إلى البحث عن مزيد من المعلومات، والبيانات التى تزيد حجم معرفته بهذه النظم، مع تلمس خفاياها المحظورة دون وجود نية مبيتة لأغراض تخريبية(٣).

إن تزايد حجم المعلومات المنتشرة على ساحة الأنترنت وتصاعد قيمتها بوصفها مصدراً معرفياً، أو اقتصادياً، أو سياسياً - بحسب طبيعة موقع

---

= هذين الاصطلاحين، ووجود الكثير من اللبس فى المفهوم بالشكل الذى نشب عنه استعمال أحد الاصطلاحين بدلاً من الآخر. وانتشر البعض الآخر بين المتخصصين فى هذا الميدان، وقد لفه غموض فى بعض جوانبه. وتشير كلمة مصدع إلى عمليات تصديع كلمات العبور، والحواجز الأمنية المعترضة، لذا أجزنا لأنفسنا إطلاق اصطلاح المصدع Cracker على كل شخص يمارس عملية تصديع كلمات العبور المصاحبة للنظم المعلوماتية، أو يباشر عملية فك الشيفرات الخاصة بحماية النظم البرمجية التطبيقية بشتى أنواعها.

ويلاحظ وجود خصوص وعموم بين هذين الاصطلاحين، فكل مصدع هو قرصان للمعلومات، أما قرصان المعلومات ليس بالضرورة أن يكون مصدعاً.

(١) أ/ حسن مظفر الرزو - مرجع سابق - ص ٧٨.

ومعنى آخر للهاكرز: بأنه متخصص فى نظم المعلومات والبرمجيات إلى حد الاتقان، بما يؤهله لاكتشاف أخطاء النظام العامل عليه وثغراته والعمل على تصحيحها. يراجع: لواء/ نجاح محمد فوزى - مرجع سابق - ص ٣٦).

(2) Paul fayler, How Ethical Hackers Pinpoint Security Weakness. Financial Times, Sep. 3, 1997, pp. 1-2.

(3) Trent, D.M., Hackers, Crackers, & Trackers, American Legion Magazine, Feb. 1997, p. 34.

Web Site الذى يحتويها – قد ألقت بظلالها على ميدان القرصنة المعلوماتية(*)، مما نجم عنه حصول تغيير فى أهداف عملية القرصنة المعلوماتية التى كانت

(*) والهاكرز كلمة تخيف الناس، خاصة مستخدمى شبكة الإنترنت، الذين يحملون خصوصياتهم الموجودة فى أجهزة الحاسب الخاصة بهم، ويبحرون بها عبر الشبكة ويعودون، وفى معظم الأحيان قد يتلصص عليهم البعض وربما استخدم هذه البيانات فى أمور غير مشروعة.

– والهاكرز باختصار هم الأشخاص الذين يلجأون بطريقة غير شرعية إلى اختراق أنظمة الحاسب الآلى بهدف سرقة أو تخريب أو افساد البيانات الموجودة بها، وفى حالة قيام المخترق بتخريب أو حذف أى من البيانات الموجودة يسمى – كراكر – لأن الهاكرز عادة يقوم بسرقة ما خفى من البرامج والملفات ولا يقوم بتخريب أو تدمير أجهزة الغير.

– ومع ظهور الإنترنت وانتشاره دولياً، أنتجت شركة IBM جهازاً أسمته – الحاسب الشخصى (P.C) الذى يتميز بصغر حجمه ووزنه الخفيف، بالمقارنة مع الحواسيب القديمة، ويتسم بسهولة نقله من مكان إلى آخر وأمكانية اتصاله بالإنترنت فى أى وقت، ومنذ ذلك الحين بدأت الحرب الحقيقية للهاكرز الذين بدأوا التسلل إلى هذه الأجهزة وسرقة المعلومات منها ومحاولة تدميرها وتخريبها، وفى بداية العقد الأخير من القرن العشرين كانت هناك حرباً حقيقية بين الهاكرز من ناحية وبين شركات الكمبيوتر والمؤسسات الاقتصادية من ناحية أخرى، حتى ألقى القبض على بعض هؤلاء الهاكرز.

– ومن أشهر هؤلاء الهاكرز – كيفين ميتسنيك – والذى قاتل المخابرات المركزية الأمريكية والمباحث الفيدرالية قتلاً معلوماتياً شرساً – وكان من شروط الافراج عن هذا الهاكرز بعد قضاء العقوبة ألا يقترب من جهاز كمبيوتر مسافة تقل عن مائة متر وذلك لأن حسب قول المراقبين والمتخصصين فى علوم الحاسب الآلى، أن لمسات أصابعه على لوحة المفاتيح كفيلة بأن تشعل حرباً عالمية ثالثة. (أنظر تفصيل قضية كيفين ميتسنيك – ص    ) من الدراسة.

– والهاكرز منهم المبتدئين، الذين تعتمد كل وسائلهم على فكرة واحدة، هى الملف اللاصق الذى يرسله المتجسس إلى جهاز الضحية عن طريق البريد الإليكترونى أو برامج المحادثة، فيقوم الأخير بفتحه بحسن نية دون دراية أنه قام فى نفس الوقت بفتح الباب على مصراعيه للتجسس لكى يدخل البريد الإليكترونى فى جهازه، وفى بعض الأحيان يمكن للمخترق أن يعمل فى جهاز الضحية ما لا يقدر عليه الضحية نفسه.

– كذلك يتم الاختراق عن طريق فحص الثغرات فى نظام الجهاز الذى يخص الضحية، حيث يرسل المخترق برنامج يسمى الخادم إلى جهاز الضحية بفتحه يصبح عرضة للاختراق، وهناك طرق أخرى للاختراق لا تحتاج ارسال برامج أو ملفات من الهاكرز ترسل إلى جهاز الضحية.

– ففى الولايات المتحدة الأمريكية أبتكرت طريقة للاختراق – عن طريق حزم البيانات التى تتدفق عبر الاتصالات الهاتفية على الإنترنت حيث يتم اعتراضها والتحكم فى جهاز الحاسب الآلى للضحية عن طريقها، وكذلك يستخدم نظام للتشغيل يسمى (unix) وهو نظام قوى

–/–

فى بداياتها عبارة عن نزعة فضولية للوصول إلى معرفة جديدة، أو تحدى العقبات الأمنية التى تضعها الجهات الأخرى لغرض الإحساس بنشوة النصر، فتوجهت صوب استثمار هذه القدرات وترجمتها إلى مكاسب مادية، أو سياسية موجهة. إذاً أضحت عملية الاختراق التى يقوم بها قرصان المعلومات تتسم بسوء قصد، وتعمد. فقد ينشأ الدافع لديه ذاتياً، أو بناءً على حافز خارجى من جهة أخرى، فيباشر عملية اعتراض سيل المعلومات المتدفقة فى الشبكة، ويحولها إلى جعبته الشخصية لكى يحقق أغراضاً مرسومة مسبقاً(١)،(*) .

---

= وصعب عن نظام (Windows) ويستخدمون أجهزة خادمة تعمل على الإنترنت وتستخدم خطوط (Ti) سريعة الاتصال بالشبكة.

- وهناك طرق وقاية كثيرة ضد عمليات الاختراق أولها تركيب برامج حماية ضد الفيروسات على جهاز الحاسب الآلى، وكذلك تشفير المعلومات المتداولة عبر الشبكة منعاً لاختراقها والاستيلاء عليها.

- راجع تقريراً بعنوان: الهاكرز - تاريخهم وبدايتهم على شبكة الإنترنت - موقع: http:// www. c4 arab. com. مشار إليه لدى. د/ عبد الفتاح بيومى حجازى - مرجع سابق - ص ٢١٥.

(1) Warren C., etal., Crime in cybercity, MCL eans, May 22, 1995, p.50.

(*) راجع: دراسة على موقع مجلة - إنترنت العالم العربى - بعنوان «موقعك فى ويب... فى مهب الاختراق»، عنوان الموقع:

- http: // www. Jaw mag. co. ae.

مشار إليها لدى: د/ عبد الفتاح بيومى حجازى - مرجع سابق - ص ٢١٧ وما بعدها.

- ومن الأمور اللافتة للانتباه أن الهاكرز بلغ مستوى النظام لديهم، أن نظمت لديهم مؤتمرات ومعارض سنوية علنية، حيث أن القانون لا يطبق على أحدهم إلا إذا ارتكب عملاً تخريبياً محدداً أو قدمت شكوى قانونية لفتح تحقيق جنائى ضده من الجهة المتضررة، وتعلم الجهات الحكومية فى الدول التى يتم فيها تنظيم مثل هذه المؤتمرات والمعارض أن نسبة كبيرة من الحاضرين قاموا بعمليات اختراق ذات طابع تخريبى، لكن لا تسمح باعتقال أىٍ منهم، إلا إذا توافرت الأدلة أو الشكوى ضده.

- وتمتاز هذه المؤتمرات بسرية هوية معظم الموجودين من زوار ومحاضرين حيث يحرص الكثير منهم على اخفاء معالمهم قدر المستطاع، فإذا قرأت الاسماء المكتوبة على لوحات التعريف الأسمية الخاصة بهم، والتى يعلقونها على صدورهم تجد أسماءً مثل - مدمر الأنظمة =/=

- و - الدكتور بروتوكول - و - صوت زحل - وأسماء أخرى غير قابلة للفهم مثل "Groopzzz".

- وأدت هذه السرية إلى ازدهار هذا النوع من المؤتمرات وانتشارها في أنحاء العالم المختلفة من ذلك مؤتمرات Chaos في ألمانيا، و Dnscon في بريطانيا و Colcon في كولومبيا، وغيرها من المؤتمرات في هولندا والولايات المتحدة الأمريكية ومن أشهر هذه المؤتمرات.

**١- مؤتمر Defecon:**

يقام هذا المؤتمر سنوياً، في مدينة - لاس فيجاس - بالولايات المتحدة الأمريكية، ويعد من أشهر المعارض الخاصة بالهاكرز، ويقام عادة في نهاية شهر يوليو من كل عام، ولم يجد المنظمون أفضل من هذه المدينة التي تقع في ولاية - نيفادا - الأمريكية، لأنها الولاية الوحيدة ضمن ولايات الولايات الأمريكية التي لا تجرم شرب الكحوليات أو لعب القمار أو احتراف ممارسة الدعارة وغيرها من المحظورات ا لتي تتم خروجاً على القانون، وفي ظل انعدام أو شبه انعدام الرقابة القانونية في هذه الولاية، يمكن تنظيم مؤتمر كهذا يجمع الهكرة من مختلف أنحاء العالم.

- وحسب - أحد منظمي المؤتمر - فإن الهدف من هذا المؤتمر ليس تعليم طرق اختراق الأنظمة - خلال بضعة أيام - بل الهدف تجميع الهكرة في مكان واحد مع العاملين المحترفين في شركات أمن الكومبيوتر والمعلومات والمهتمين في هذا المجال من قبل الحكومة حتى يتبادل الجميع خبراتهم.

- ولالقاء الضوء على نجاح مثل هذه المؤتمرات فإن المؤتمر التاسع بلغ عدد الحضور فيه عدة آلاف مقابل (٧٥) فرداً في المؤتمر الأول، وأن الزائر الواحد يسدد (٥٠) دولار أمريكي حتى يمكنه الدخول.

- ومن أسباب نجاح هذا المؤتمر، أن منظميه لاحظوا أن الغالبية العظمى من المراهقين وطلاب الجامعات، فأضافوا للمؤتمر عدداً من الفقرات الترفيهية كالحفلات الموسيقية وهذه الفقرات قد تنطوي على بعض النشاطات غير القانونية التي لا يسمح بها في غير مدينة لاس فيجاس، وذلك في محاولة لجذب أكبر عدد من هؤلاء الهكرة، واقناعهم بالتخلي عن الحذر الشديد وتقديم خبراتهم إلى العالم.

وحتى نعرف ما دار في المؤتمر السابع على سبيل المثال، يمكن تصفح عناوين المحاضرات التي ألقيت في هذا المؤتمر ومنها.

- كيف تكتشف إذا كان الشخص الواقف أمامك يعمل مع الحكومة؟
- المحاضر (هاكر مجهول الهوية).
- الأخطاء الشائعة عند توظيف الهكرة في أعمال نظامية، المحاضر (مدير شركة).
- الثغرات الأمنية في أنظمة ماكنتوش، المحاضر (موظف سابق في شركة أبل).
- كيف تساهم الفيروسات في زيادة أمن الأنظمة، المحاضر (مؤلف فيروسات).
- علاقة الهكرة بالأعلام، المحاضر (صحفي).

-/-

والقراصنة يمكن تصنيفهم إلي ثلاثة أنواع[1]:

( أ ) من يطلق عليهم ذوى القبعات البيضاء: وهم الذين يهاجمون أجهزة

---

-- - صناعة الأسلحة التى تعتمد على الترددات الراديوية عالية الطاقة، المحاضر (هاكر مجهول الهوية).

- مزودات بروكسى المضادة للرقابة، المحاضر (خبير فى أمن الشبكات).

- الهكر الأخلاقى والوطنية، المحاضر (ضابط فى الجيش الأمريكى).

- اختراق العقل البشرى، المحاضر (طبيب نفسى).

- وبالإضافة إلى ما تقدم فقد كان الجديد بالمؤتمر ما أعلنته جمعية تعمل فى - مجتمع إنترنت السفلى والتى تعرف باسم «طائفة البقرة الميتة Cult of the dead cow»، عن قيامها باطلاق برنامج Back crifice 2000 ويعرف اختصاراً بـ BO2K وهو أحد أشد البرامج المستخدمة لاختراق الأنظمة فى العالم إن لم يكن أشهرها، الأمر الذى لاقى تصفيقاً حاداً من الجمهور.

٢- مؤتمر Hope:

كان أولى اجتماعاته فى عام ١٩٩٤، ويقام كل ثلاث سنوات فى مدينة - نيويورك - وقد نظمت مجلة - ٢٦٠٠ - ربع السنوية، المختصة بالهاكرز، هذا المؤتمر عام ١٩٩٤ وعام ١٩٩٧، وعام ٢٠٠٠، حيث خصص المؤتمر الأخير لبحث مشكلة الألفية أو العنصرية كما أطلق عليها فى حينه، على حين أن المؤتمرات السابقة ركزت على الجوانب الأمنية لأنظمة الاتصالات.

- وهذا المؤتمر أكثر انضباطاً من مؤتمر Defcon وأكثر التزاماً بالشرعية والقانون، وذلك لاحتمال أن منظميه يشعرون بجدية القوانين المضادة للهكر، حيث يقومون بحملة تطالب باطلاق سراح Kevin Mitnick أحد أشهر الهاكرز بالعالم (والذى سوف نعرض لقضيته فى مجال اختراق أمن المعلومات فيما بعد). والسبب فى التزام هذا المؤتمر بالقانون أن قوانين الولاية التى يقام فيها المؤتمر هى أكثر تشدداً من قوانين ولاية نيفادا الأمريكية.

٣- مؤتمر Sammercon:

وهو مؤتمر سنوى تنظمه مجلة Root and phrack فى مدينة - أتلانتا - الأمريكية، ويمكن لأى راغب فى الحضور لهذا المؤتمر أن يشارك مجاناً عدا الصحفيين حيث يسدد الصحفى رسم دخول قدره (١٠٠) دولار، ويسدد العاملين فى الحكومة رسماً قدره (٥٠٠) دولار عن المشارك الواحد وقد أثبتت هذه المؤتمرات أنه لابد من التعامل مع الهكرة والاستماع إلى آرائهم وتبنى أبتكاراتهم القائمة فى قطاع أمن الشبكات والمعلومآت والاستفادة منها، ولابد كذلك من التعرف على آخر ابتكاراتهم واختراقاتهم لاتخاذ اجراءات الحماية منها وهذا ما تقوم به الشركات الخاصة - راجع دراسة بعنوان - منظمات الهاكرز وتجمعاتهم - على شبكة الإنترنت وعنوانه .http: // www. dit net. co. ac.

(١) لواء د/ محمود وهيب السيد - مرجع سابق - ص ٣٢.

الكومبيوتر بطريقة شرعية وبأوامر من السلطة وبهجمات مخططة وينظمون الهجوم عندما يطلب منهم ذلك.

(ب) من يطلق عليهم ذوى القبعات الرمادية: وهم من يقومون بالهجوم كقراصنة أشرار وأحياناً لهدف آخر، وبعضهم يؤمن بنظرية حرية المعلومات أياً كانت هذه المعلومات، بما فيها التى تتعلق بتأمين الأجهزة والشبكات ومعرفة نقاط الضعف، ولا يرون غضاضة فى الهجوم على أى موقع من أجل المزيد من إجراءات الأمن والوقاية، وهذا النوع فى ازدياد مستمر ويقوم به كل من يجد فى نفسه الكفاءة فى استخدام الكومبيوتر، وهؤلاء يطلق عليهم Hrackers والذين قد تكون أعمالهم للهواية فقط أو العمل الضار أصلاً لتخريب مواقع هامة أو شراء بعض المنتجات والبرامج بطرق ملتوية، وللحصول على معلومات هامة من أماكن مختلفة وأخطرهم صانعو الفيروسات وملفات كسر الحماية، وهناك فئة أخرى يطلق عليها Crackers وهم مستخدمون عاديون أو هواة لديهم القدرة على البرمجة والبحث الجيد على صفحات الإنترنت، للوصول إلى ملفات كسر الحماية بغرض إستعمالها أو النسخ غير الشرعى للبرامج.

(جـ) من يطلق عليهم ذوى القبعات السوداء: وهؤلاء يهاجمون نظام المعلومات بهدف سطو مالى أو معلوماتى ضار يحقق لهم نفعاً ما.

ومن أمثلة الهاكرز المحترفون، نستعرض وقائع الفكر الإجرامى لخرق نظم أمن المعلومات فى قضية الجانى فيها يدعى (إبراهيم عبد الله)..

– حين وصل ا لثامنة عشر بدأ حياته الإجرامية مبكرة وكانت هوايته تزوير بطاقات الائتمان البنكية واستطاع سرقة أرقام – ٨٠٠ – كارت ائتمان وحوالى مائة ألف دولار، كما قام بسرقة أرقام بطاقات الائتمان من زبائنه فى المطعم الذى يعمل به، وتم القبض عليه ومحاكمته فى هذه القضايا وقضية أخرى فى – جزر ڤيرجين – حين حاول سرقة بعض الأشخاص والاحتيال عليهم.

– وحين خرج من السجن وجد ضالته فى مجال الإنترنت وتكنولوجيا المعلومات، وأصبحت هوايته المفضلة هو الجلوس أمام شاشة الكومبيوتر واستخدام شبكة الإنترنت من خلال كمبيوتر مكتبة صغيرة فى حى – بروكلين – فى نيويورك، وقد تمكن من الحصول على قائمة مجلة – فوريز – التى تضم أشهر (٢٠٠) شخصية وأغناها فى الولايات المتحدة، وبدأ فى اعداد خطة محكمة من أجل سرقتهم والاحتيال عليهم(١).

وقد وضع – ابراهيم عبد الله – خطة محكمة للايقاع بهؤلاء، إذ بالحصول على قائمة – فوريز – وسع نشاطه بشكل ملحوظ، وبدأ عملياته الأولى بخداع الشركات مثل – أرد بليوو.أكويناكس وأكبيريان – واستطاع بذلك تزوير تقارير الائتمان الخاصة بضحاياه من المشاهير والأغنياء، واستخدم المعلومات السرية والتقارير الخاصة بهؤلاء، للحصول على معلومات فى شأن هوياتهم، ودخل إلى حساباتهم البنكية واستولى منها لنفسه على مبالغ مالية ضخمة.

– وكان من المستحيل الوصول إليه بسبب الاحتياطات والخدع التى مارسها، إذ مارس كل هذا النشاط والذى يوحى لدوائر الشرطة أنه خارج نيويورك على حين أنه داخلها، بل كان يمارس هذا النشاط من مطبخ المطعم الذى يعمل فيه، واستعان بهاتف محمول مرتبط بالإنترنت وكان يبعث رسائله إلى ضحاياه عن طريق زملائه من الطهاة والخدم فى ذلك المطعم، بل أنه تخير أحدهم وهو – مايكل يوجليس – الذى أصبح ساعده الأيمن، واكتسب منه خبرة فائقة فى أسلوبه الإجرامى المعلوماتى.

– وكانت الهفوة التى أسقطته فى يد الشرطة فى ديسمبر عام ٢٠٠٠ حين أرسل طلباً بالبريد الإليكترونى إلى مؤسسة – نظم سيبيل العالمية – والمشهورة

---

(١) نص قضية (الهاكر) ابراهيم عبد الله، منشورة تفصيلاً لدى مجلة – أخبار الحوادث – المصرية الصادرة عن دار أخبار اليوم، العدد رقم ٥٠٨، السنة التاسعة، الخميس ٢٠٠١/١٢/٢٧، ص ص ٢٠-٢١.

فى مجال الاستثمارات، وكان موجهاً إلى - يدل ليدشن - مدير المؤسسة، وذلك بطلب تحويل عشرة ملايين دولار من رصيد - توماس سيبيل - منشأ هذه المؤسسة إلى رصيد جديد له فى استراليا، وكان من شأن تحويل هذا المبلغ، الاخلال بالتوازن المالى للمؤسسة فأوقف تحويل هذا المبلغ إليكترونياً، وتم الاستفسار من مؤسس الشركة لدى استراليا، الذى نفى أنه قدم هذا الطلب، وعلى الفور أبلغت المباحث الفيدرالية التى فحصت كل من له مصلحة فى تزوير طلب التحويل المذكور، وكان ضمن المشتبه فيهم - ابراهيم عبد الله - الذى قبض عليه، وبحوزته بعض أدلة الاتهام ومنها أجهزة تزوير كروت الائتمان، وسجلات حسابات، وكراسات صغيرة وطوابع مطاطية بها صور المشاهير المذكورين، وعناوين محال اقامتهم وكذلك بيانات أخرى عنهم، منها تواريخ الميلاد الخاصة بهم.

- وقد صنف الخبراء المختصون هذا - الهاكر - بأنه عبقرى فى حل الشفرات وتزوير كروت الائتمان، فهو خبير كمبيوتر وإنترنت محترف وعبقرى، وقال المجنى عليهم من الهاكر المذكور أنهم لم يشعروا بأفعال السرقة والاحتيال أو وقوع شئ غير عادى بالنسبة لهم عند ممارسة الجانى لسلوكه غير المشروع(١).

- **قضية الهاكر كيفين ميتسنيك:**

- تعرف - كيفين - إلى مجموعة أخرى من الشباب لها ذات الاهتمام بالمعلومات والهواتف والحاسبات وشكلوا عصابة هدفها اقتحام الهواتف الخاصة بأى جهة والتلاعب كيفما شاءوا فى البدالة الخاصة بها - تحويلة التليفونات - وكانوا يتقمصون شخصية موظف التليفونات، ويردون على صاحب الهاتف، باجابات مازحة منها الرقم المطلوب، خمسة، إثنان، ثلاثة ونصف... كيف تستطيع أن تطلب النصف؟ وفى مكالمة أخرى يردون على الهاتف بأن الحرارة

---

(١) راجع دراسة على موقع انترنت العالم العربى - بعنوان «موقعك فى ويب... فى مهب الاختراق» - مرجع سابق - وعنوانه .Sjttp:// www. jawmag. co. ac.

سوف تقطع ما لم يسدد صاحب الرقم عشرين سنتاً وهكذا كانت مكالمات وردود هؤلاء هدفها التسلية لهؤلاء الشباب(١).

- وفى عام ١٩٨١ دخل - كيفين - وإثنان من مجموعته إلى المركز الرئيسى لشركة الهاتف فى مدينة - لوس أنجلوس - ووصلوا لغرفة الكومبيوتر الذى يتحكم فى عملية الاتصال، واستولوا على كتب التشغيل الخاصة به وقوائم وسجلات تتضمن مفاتيح السر لأقفال الأبواب، وذلك فى تسعة مراكز أساسية تابعة لشركة الهاتف فى المدينة، وتمكن أحد هؤلاء من تدمير ملفات إحدى شركات الكومبيوتر فى - سان فرانسيسكو - بسبب المعلومات التى حصل عليها مع (كيفين).

- ولم تستطع الشرطة الوصول إلى الفاعل، وبعد عام، وبناءً على وشاية من فتاة ضمن مجموعة - كيفين - ألقى القبض عليه وزميلين، وقضى ضدهم بالحبس ثلاثة أشهر، وأودعوا سجن الأحداث بتهمة السرقة، وتدمير بيانات عبر شبكة كمبيوتر، كما أمرت المحكمة بعد ذلك بوضعه لمدة سنة تحت مراقبة الشرطة فى لوس أنجلوس.

- من جهة أخرى فإن مراكز الخدمة الاجتماعية حاولت تأهيل - كيفين - ومساعدته بوصفه حدثاً جانحاً، ومريضاً، وليس فى حاجة للعقوبة بقدر ما هو فى حاجة إلى التأهيل والعلاج، ولذلك حاولت هذه المراكز الاستفادة من خبراته فى مجال الكومبيوتر والاستفادة منها بشكل شرعى، لكن سرعان ما حاول - كيفين - تعلم حيل مختصرة الهدف منها اختراق شبكات الكومبيوتر، ولذلك ضبط من قبل شرطة - جامعة شمال كاليفورنيا - حيث كان يحاول اختراق شبكة A.R.P.A net، وذلك للوصول من خلالها إلى وزارة الدفاع الأمريكية

---

(١) راجع فى قضية - كيفين ميتسنيك - كاملة ما نشر بمجلة إنترنت العالم العربى عام ١٩٩٨، تحت عنوان كيفين ميتسنيك الماكر الأكبر - نسر ينقض على شبكات الكومبيوتر، فى جزئين - على موقع: http: // www. ditnet. co. ae.

(البنتاجون) وقضى ضده بالتدريب لمدة - ستة شهور - فى اصلاحية للأحداث فى كاليفورنيا.

- وبعد عدة سنوات أخرى، قبض على - كيفين - بتهمة اختراق حاسب آلى خاص بإحدى الشركات، وقد بقى رهن الاعتقال لمدة سنة كاملة، وبدون محاكمة، وفى الوقت نفسه اختفى ملف - كيفين - من مركز الشرطة دون تفسير أو مبرر لاختفاء هذا الملف.

- وفى عام ١٩٨٧ ضبط - كيفين - وهو يحاول سرقة - برامج - من إحدى شركات البرمجيات وذلك عن طريق شبكة الإنترنت، وتمكنت شرطة كاليفورنيا من تتبعه من خلال خط الهاتف الذى يتصل منه، وتوصلا للشقة التى يعيش فيها فى كاليفورنيا، ووضع تحت المراقبة لمدة (٣٦) شهراً، وترتب على ذلك أنه زاد فى نفسه الاحساس والشعور بالعظمة والقدرة الفائقة على الآخرين، ولم يمكنه الوضع تحت المراقبة من الخلاص من هذا الشعور(١).

- وفى عام ١٩٨٨، صمم - كيفين - على ضرورة الحصول على نسخة من نظام تشغيل - الميني كمبيوتر - من إنتاج شركة ديجيتال، وذلك عن طريق اختراق شبكة - إيزى نت - الخاصة بالشركة، ولهذا الغرض، كان - كيفين - يذهب مساء كل يوم إلى صديقه - ديبجو - والذى يعمل فى قسم دعم البرامج فى إحدى شركات الكومبيوتر، وكانا يحاولان لساعات طويلة الدخول إلى شبكة شركة - ديجيتال - واكتشف المسئولون هذه المحاولات للاختراق، واستعانت الشركة بالشرطة المحلية، ومكتب التحقيقات الفيدرالى، وعملاً بالتعاون مع خبراء شركة ديجيتال محاولين - دون جدوى - ولعدة أيام التوصل لمصدر الاختراق، وذلك دون نتيجة، بسبب الاجراءات الاحتياطية والذكية التى اتخذها - كيفين - ومنها:

---

(١) راجع قضية - كيفين ميتسنيك - على الموقع السابق لمجلة إنترنت العالم العربى، عام ١٩٩٨.

١- استخدم - كيفين - جهازى حاسب آلى، الأول يحاول منه اختراق شبكة شركة ديجَيتال، والثانى يراقب به رد فعل شركة ديجيتال والشرطة التى تحاول الوصول إليه وذلك عن طريق مراقبة مركز مؤسسة الهاتف.

٢- كذلك فإن - كيفين - تحسب لإمكانية التوصل إليه عن طريق الهاتف الذى يتصل منه، وذلك لأنه عبث ببدالة شركة الهاتف - المحول التليفونى - ولهذا عندما سارعت الشرطة للقبض عليه فى الشقة التى يوجد بها رقم التليفون الذى يتصل منه، تبين للشرطة أنه تم تضليلها بسبب التلاعب فى أرقام التليفونات.

- ورغم مئات الآلاف من الدولارات التى أنفقت من قبل شركة - ديجيتال - للقبض على (كيفين)، ورغم جهود الشرطة المحلية والمباحث الفيدرالية الأمريكية، لم تتمكن من القبض عليه، لكن فى مرحلة لاحقة وبناء على بلاغ من صديقه - دييجو - أمكن للشرطة القبض على كيفين، وذلك رداً على وشاية - كيفين - ضد صديقه دييجو، لشركته التى يعمل بها بأن لديه متاعب مع مصلحة الضرائب، ووجد - كيفين - نفسه مقبوضاً عليه فى قضية سرقة برامج كمبيوتر قيمتها ملايين الدولارات، فضلاً عن تسببه فى خسارة شركة - ديجيتال - لأكثر من ٢٠٠ ألف دولار صرفت من قبل الشركة لأجل اكتشافه والقبض عليه، كما وجهت إليه لدى محكمة - لوس أنجلوس - تهم استخدام الكومبيوتر سنوات طويلة فى الاحتيال، وحصوله على كلمات السر، لأجهزة الكومبيوتر الخاصة بعدد من الشركات، وذلك بشكل غير مشروع.

- وقد كان الحكم الذى صدر ضده مثيراً للرأى العام فى الولايات المتحدة الأمريكية حيث قضى ضده بالحبس لمدة سنة، وبالعلاج لمدة - ستة شهور - من إدمان اختراق نظم الكومبيوتر عبر الشبكات(*).

---

(*) لذلك فقد نبه هذا الحكم إلى أن الحدث أو الشاب يمكنه أن يصل إلى مرحلة - الادمان - فى استعمال الكومبيوتر والإنترنت، وهو أمر يجب أن تلتفت إليه سلطات التحقيق والمحاكمة

=/=

– وفى بداية التسعينات من القرن الماضى، فإن – كيفين – وبعد أن أمضى فترة العقوبة، لم يلتزم بالبقاء فى لوس أنجلوس من أجل التأهيل، إذ غادرها إلى مدينة – لاس فيجاس – وعمل مبرمجاً لدى إحدى الشركات التى تعمل فى مجال القوائم البريدية الإليكترونية.

– وفى عام ١٩٩٢، عاد إلى سان فرانسيسكو، وعمل مع والده فترة بسيطة فى أعمال البناء، ثم عمل لدى – وكالة تحقيق – وبعد فترة بسيطة اكتشفت عملية استخدام غير شرعى لقواعد البيانات التى تملك وكالة التحقيق المذكورة الدخول إليها، وأشارت أصابع الاتهام إلى كيفن، الذى فتش منزله بحثاً عن أدلة فى شأن اتهامه بإستخدام غير مشروع لقواعد البيانات، ولذلك فإن قاضى التحقيق وجه إليه تهمتين الأولى هى الدخول غير المشروع إلى كمبيوتر إحدى الشركات، والثانية كسر مدة المراقبة المفروضة عليه كعلاج نفسى، وإزاء ذلك هرب من سان فرانسيسكو، ولم تعثر الشرطة عليه.

– وفى ديسمبر عام ١٩٩٢، تلقى قسم الآليات فى كاليفورنيا اتصالاً بطريق الكومبيوتر، ويطلب فيه صاحبه نسخ من شهادات رخص قيادة لأولئك المتعاونين مع الشرطة، واستخدم المتصل – شفرة – تظهر أنه مخول قانوناً بالاطلاع على هذه الوثائق، وطلب موافاته بها بطريق الفاكس، وذلك فى عنوان بإحدى ضواحى لوس أنجلوس. وقد استشعر مسئولوا الأمن بدورهم الريبة فى الطلب، وتبين أن رقم الفاكس يخص محل لتقديم خدمات التصوير والفاكس وقام الأمن بإرسال صورا لأوراق المطلوبة إلى ذات عنوان الفاكس، لكن الأمن أرسل عناصر منه إلى ذات العنوان لرصد مستلم هذه الأوراق، ولم يرونه إلا وهو خارج من المحل الذى تسلم منه الأوراق وفشلوا فى القبض عليه، وألقى الأوراق

---

والتأهيل فى قضايا – انحراف الأحداث – التى يكون سببها الكومبيوتر والإنترنت، وذلك لظهور ما يسمى بالهوس الإنترنتى أو الاجرام الإنترنتى.

التى تسلمها، وعند فحصها تبين أنها تحمل بصمات – كيفين – الذى لازال يمارس نشاطه[1].

– وإزاء فشل الأمن فى القبض على – كيفين – اهتمت الصحافة بأخباره، وتخصص أحدهم ويدعى – ماركوف – فى أخباره وحاول أن يلتقط كل الأخبار فى خصوصه لدرجة أن مكتب التحقيقات الفيدرالى جنده كمستشار فى عمليات مطاردة – كيفين – للقبض عليه، وذلك فى أعياد ميلاد عام ١٩٩٤.

– والذى حدث فى عام ١٩٩٤، أن المدعو – شيمو مورا – وهو خبير فى أمن الشبكات والبرمجة، بل أشهر خبراء أمن الشبكات والبرمجة، ويعمل مستشاراً لمكتب التحقيقات الفيدرالى، والقوات الجوية، ووكالة الأمن القومى الأمريكية، حيث يعمل كذلك مطوراً لبرامج الكومبيوتر الخاصة بحماية نظم شبكات الكومبيوتر من الاختراق، وهذه الأسطورة فى عالم الكومبيوتر، أُخطر من قبل معاونيه أن – الكومبيوتر الشخصى – الخاص بمنزله والمتصل بشبكة العمل الواسعة، تعرض للاختراق، فقطع – شيمومورا – أجازته وعاد فوراً كى يبحث عمن اقتحم – عرين الأسد – بلغة الغابة، لأنه لم يعتقد على الاطلاق أن يجرؤ أحدهم على اقتحام الكومبيوتر الخاص به.

– وكان – شيمومورا – قد طور وركب نظام مراقبة، يرسل انذاراً بمحاولة اختراق لشبكة الكومبيوتر التى تتصل بها أجهزة الحاسب الآلى المنزلية الخاصة به، وهو أمر لم يتنبه له (كيفن)، والذى حدث أن محاولات – كيفين – للاختراق سجلت وأرسلت آلياً إلى جهاز أخر مرتبط بذات شبكة – شيمومورا – ومكن ذلك أعوانه من طرد كيفن، وفى الوقت ذاته مكن – شيمومورا – من دراسة الهجوم وتتبع مصدره، لكن سرعان ما اكتشف هو والشرطة أن مصدر الاتصال كان زائفاً – إذ بدا على غير الحقيقة – وكأنه قادم من إحدى جامعات شيكاغو.

---

(١) راجع سرد قضية – كيفين – على شبكة الإنترنت، الموقع السابق.

– ولم يكف – شيمومورا – عن مطاردة – كيفن – وذلك بمعاونة مكتب التحقيقات الفيدرالية، إذ بفضل جهوده وبسبب نظم المراقبة التى طورها، تمكن من تتبع هذا المعتدى وهو يتلاعب ببدالات شركات الهاتف – تحويلات التليفون – ويسرق ملفات من شركة – موتورالا – للاتصالات، وشركة – أبل – للكومبيوتر التجارية، ودارت الشبهات حول – كيڤن – الذى أختفى عن الأنظار عام ١٩٩٢ ، وثبت أنه يقوم بنشاطه الإجرامى – عبر شبكة هواتف متحركة – من مدينة (رالى) فى شمال كاليفورنيا.

– وفى يوم الأحد ١٣ فبراير ١٩٩٥ طار – شيمومورا – إلى مدينة رالى، وفى اليوم التالى، تمكن خبراء الهاتف المحلية والمحققين الفيدراليين عن طريق استخدام ماسحة لتردد الهاتف المتحرك، حيث حدد مكان – كيڤن – بدقة، وفى مساء ١٥ فبراير ١٩٩٥ تم القبض على كيڤن فى الشقة رقم (٢٠٢) باحدى ضواحى مدينة (رالى) متلبساً باختراق إحدى الشكبات[(١)] .

– وبعد اعتقال – كيڤن – وضع فى السجن بدون محاكمة، حيث حكم عليه فى ١٧ يونيو ١٩٩٧ ، بالسجن لمدة (٢٢) شهراً، كان كيڤن قد قضاها رهن الاعتقال، ومع ذلك لم يفرج عنه بعد انتهاء العقوبة فى انتظار محاكمات أخرى، وحجة سلطات الأمن فى ذلك، أن – كيڤن – من الخطورة، بحيث أنه باتصال هاتفى واحد، يمكن له وضع البلاد فى حالة استنفار قصوى، قد تؤدى لحرب عالمية ثالثة، وذلك بسبب قدرته الفائقة على اقتحام أخطر مواقع من خلال شبكات الكومبيوتر والهاتف (الإنترنت)[(٢)] .

---

(١) راجع قضية، كيڤين ميتنيك، المرجع السابق، ذات الموقع على شبكة الإنترنت.

(٢) راجع فى شرح قضية – كيڤين – كاملة لدى، د/ ممدوح عبد الحميد المطلب – فى مؤلفه – عن جرائم استخدام الكومبيوتر وشبكة المعلومات العالمية (الجريمة عبر الإنترنت) – دار الحقوق – الشارقة – الإمارات العربية، عام ٢٠٠١، ص ص ١٦١ – ١٦٩ . وراجع كذلك معلومات عن كيڤن على شبكة المعلومات العالمية – إنترنت – موقعاً باسم كيڤن "www. Kevinmitnick. com".

–/–

## المبحث الثاني

## وسائل حماية المعلوماتية

**• أهمية توفير الحماية للمعلوماتية:**

من الضروري بسط وسائل الحماية لنظم المعلوماتية، حيث أن ذلك من الناحية الشخصية يحقق أمن المعلومات المتعلقة بأسرار أفراد المجتمع فى مواجهة نشرها، والعبث بمكنونات الإنسان عبر وسط تقنى لا يرحم، ومن الناحية الموضعية فإن توفير الحماية المعلوماتية ينطوى على تأمين الاستثمارات المادية والبشرية المستخدمة والمستثمرة فى مجال تكنولوجيا المعلومات، كما أن هذه الحماية تشجع ذوى العقول النيرة على أطلاق ابداعات الابتكار مع حفظ حقوهم الفكرية، كما تدفع حماية النظم المعلوماتية عجلة التقدم العلمى والتقنى فى اتجاه الامام للرقى بالمنظومة التعليمية والتنموية والاقتصادية للدولة، بما يحقق أهداف الانفتاح الاقتصادى على العالم الخارجى، وتطبيق فكر العولمة Globalization فى جانبه الايجابى المفيد للآليات الوطنية.

**أولاً: أهمية الحماية المعلوماتية على المستوى الشخصي:**

تفضى حماية نظم المعلوماتية إلى صيانة وحفظ المعلومات المودعة فى الحاسب الآلى، والتى قد يؤدى نشرها إلى شيوع معرفة جوانب شخصية، وتعريض أسرار الحياة الخاصة للفرد لخطر محدق، ولا شك أن برامج الحاسب قد تنطوى على معلومات تم تجميعها وحفظها، وحماية هذه البرامج تحول دون

---

= وهذه المعاملة القاسية التى يواجه بها - كيفن - زادت عدد المتعاطفين معه الذين يطالبون بالإفراج عنه فوراً، بوصف أنه ليس مجرماً، ولم يبع المعلومات والبرامج التى كان يستولى عليها، وكان يستخدمها فى زيادة قدراته. وهذا النظر يتفق مع حكم محكمة لوس أنجلوس ضده عام ١٩٨٨، حيث قضى ضده بالسجن لمدة سنة واحدة، وستة شهور معالجة من - إدمان اختراق نظم الكومبيوتر عبر الشبكات - مؤدى ذلك أنه مريض بما يسمى بالهوس الإنترنتى، أو ما يطلق عليه الاجرام الإنترنتى، وذلك لأن مثل هذه الحالات فى حاجة للعلاج وليس العقاب.

تفاقم أخطار استعمال المعلوماتية بشكل سلبى يهدد الحياة الخاصة وأسرار الإنسان الشخصية.

كما أن بعض البرامج قد تقوم على تغيير بعض البيانات التى تم تخزينها من قبل فى الحاسب الآلى، وإحداث غش فيها أو إتلاف برامج أو التجسس على ما تحتويه من معلومات... أو ما إلى ذلك من وقائع إجرامية، لذلك شرعت الدول المتقدمة – دول العالم الأول(*) – ذات النظم القانونية العريقة، باحداث تعديلات تشريعية وسن قوانين تهدف لحماية الحياة الخاصة للأفراد، واعتباراً من سبعينات وثمانينات ا لقرن الماضى بدأت مواجهة هذه الأشكال المستحدثة من الإجرام المعلوماتى – الجريمة الافترضية – وتأكيد حماية حقوق الملكية الفكرية – والأدبية – التى يتمتع بها الأفراد، والحيلولة دون الاعتداء على هذه الحقوق، باستغلال التيسيرات التى توفرها التقنية المعلوماتية، وهكذا فإن حماية نظم المعلوماتية وبرامج الحاسب الآلى، تعد خطوة هامة وعامل مؤثر فى سبيل صيانة الحياة الخاصة للفرد.

إن المعلومات المخزنة فى الحاسب الألى يجب أن تكون بمنأى عن أى اعتداء، وإلا انتهكت الأسرار الخاصة لحياة الأفراد، وعلى سبيل المثال فإن حسابات الأفراد فى البنوك تسجل فى حاسب الآلى تقيد به جميع العمليات التى يقومون بها ووقتها وأطرافها، وهذه المعلومات يمكن نقلها من خلال وسائل تكنولوجية تمكن من إيجاد شبكة معلومات تسهل للأشخاص الأطلاع على هذه العمليات(١). ولذا يجب حماية المعلومات الشخصية للأفراد من هذه المخاطر.

---

(*) قياساً على أنه مازال يطلق على الدول النامية وصف دول العالم الثالث، فهذا الوصف بحق خاطئ، وذلك التقسيم لاشك ظالم. فقد نهضت دول عديدة من غفوتها وتقدمت وزاحمت دول المقدمة، ومازال التقدم التنموى مستمر.

(١) د/ طارق أحمد فتحى سرور – الحماية الجنائية لأسرار الأفراد فى مواجهة النشر – دار النهضة العربية – سنة ١٩٩١ – ص ٢٠٤.

● أصبح التوصل إلى البيانات والحقائق عن الأفراد أكثر سهولة من ذى قبل بفضل الحاسب الآلى، =/=

ووفقاً للقانون رقم ٣٥ لسنة ١٩٦٠ فى شأن الإحصاء والتعداد – المعدل بالقانون رقم ٢٨ لسنة ١٩٨٢، تعتبر البيانات الفردية التى تتعلق بذلك بيانات سرية ويعاقب القانون على الإخلال بسرية هذه البيانات الفردية أو إفشائها. وذهب رأى(١) إلى أن ذلك ليس كافياً، لأن التوسع فى استخدام الحاسب الآلى، يستلزم حماية تشريعية فعالة لأسرار الأفراد التى يتم حفظها فى برامج الحاسب، وإنه لابد من نصوص واضحة تجرم الانحراف بالمعلومات أو إفشائها، إذا كان فى ذلك مساس بسمعة الشخص أو حرمة حياته الخاصة، سواء تم ذلك عمداً أو نتيجة أهمال كما نص على ذلك القانون الفرنسى الصادر فى ٦ يناير سنة ١٩٧٨م، وكما نصت المادة ٥٥٢ (أ) من قانون سنة ١٩٧٤ بشأن الخصوصية، التى نصت بأنه لا يجوز لأية جهة أن تنشئ معلومات يتضمنها نظام معلوماتى بأى وسيلة من وسائل الاتصال لأى شخص أو لأى جهة أخرى ما لم يكن ذلك بناء على طلب كتابى بموافقة صاحب الشأن الذى تتعلق به المعلومات، باستثناء الإفشاء الذى تقتضيه المصلحة العامة، أو الذى يتم بأمر المحكمة.

**ثانياً: أهمية الحماية المعلوماتية من الناحية الموضوعية:**

حماية برامج المعلوماتية، يفضى من الناحية الموضوعية إلى تشجيع الأفراد على ابتكار البرامج التى تسهم فى الاثراء العلمى والتقنى للدول ويحقق تقدمها الاقتصادى، فضلاً عما يعود لهؤلاء من فوائد جمة من جراء ذلك، كما تقضى هذه الحماية على نشاط القرصنة الدولية لاختراق البرامج والنظم.

---

= وقد أدى ذلك إلى زيادة الحاجة إلى اتخاذ الحيطة اللازمة للمحافظة على أسرار الأفراد. وفى صدد هذه المشكلة توجد مشكلتان فرعيتان:

**الأولى:** تتعلق بالكمبيوتر كوسيلة تكنولوجية لجمع المعلومات التى تهدد حرمة الحياة الخاصة.

**الثانية:** تتعلق باستعمال المعلومات المودعة فى الكمبيوتر بما يتضمنه من نشر لأسرار الحياة الخاصة الكامنة فى هذه المعلومات.

(١) رأى د/ طارق أحمد فتحى سرور – المرجع السابق – ص ٢٠٨.

أ - إن حماية نظم المعلومات تشجع علي الابتكار:

إن حماية برامج نظم المعلومات تشجيع الأفراد على الابتكار، وولوج عالم تأليف البرامج التى تساعد على تقدم الأمم علمياً وتكولوجيا؛ ذلك أن المبرمج المبتكر سينال مقابلاً عادلاً لجهده، فيحيا حياة كريمة، تدفعه إلى الإمعان فى التعمق فى الابتكار حتى ينال مقابلاً جديداً، «وإلا فما حاجة أى شخص للابتكار إذا كان مآل عمله إلى الاستغلال المجانى من الجمهور»(1).

كذلك فإن حجم الاستثمارت والميزانيات التى يتم استخدامها للإنفاق على إنتاج الأموال المعلوماتية كبير ويمس مصالح كثير من الشركات والبنوك(2)، فإذا لم يتم حماية نظم المعلومات، فإن ضياع هذه الأموال يؤدى إلى إحباط شديد ينجم عنه قتل روح الإبتكار عند الأفراد والأشخاص المعنوية، التى تنفق بسخاء من أجل الارتفاع بمستوى حياة الأفراد اقتصادياً واجتماعياً وعلمياً وخلقياً، فبرامج المعلوماتية هى برامج حياة وبرامج لصناعة المستقبل، من خلال كم الابتكار الذى تنطوى عليه والذى تفيد منه البشرية، فى صناعة مستقبلها فضلاً عن حصول الأفراد والأشخاص المعنوية على مقابل مجز لذلك، يشجعهم على الاستمرار فى مواصلة تقدمهم، وإلا فإنه إذا لم يحصل الأفراد والأشخاص المعنويون على سعر مناسب لما بذلوه من جهد، فإن ذلك سيدفعهم إلى الامتناع عن بذل جهد ابتكارى فى مجال تأليف برامج الحاسب الآلى.

والدول النامية قد تكون فى حاجة إلى الإفادة من البرامج التى يمكن أن تصل إليها، بيد أنها عندما ترقى ستجد أن برامجها هى نفسها محلاً للاعتداء عليها من جهات أخرى، ويصبح التقدم له حقاً للمبتكرين بل وقفاً على المعتدين، ولذا فإن عدم تكريس الحماية الجنائية لبرامج نظم المعلومات قد يوفر البرامج فى

---

(1) د/ محمد حسام محمود لطفى - الحماية القانونية لبرامج الحاسب الآلى - دار الثقافة للطباعة والنشر - القاهرة - سنة 1987 - ص 34.

(2) د/ هدى حامد قشقوش - جرائم الحاسب الآلى - مرجع سابق - ص 70.

الأسواق العالمية بأسعار زهيدة، لأنها برامج مقلدة لا تكلف سوى ثمن الدعامة التي يسجل عليها البرنامج، ولكن ذلك سيؤدى إلى توقف عمليات الإبداع العالمى فى مجال ابتكار البرامج، وهكذا فإن حماية برامج الحاسب الآلى تساعد على تشجيع روح الابتكار لدى الأفراد والدول، وخيراً للأفراد وللدول أو تشترى البرنامج الصحيح بمئات الجنيهات وتسهم فى التقدم العالمى المشروع من أن تشترى برنامجاً مقلداً ببضعة قروش[1] وتسهم فى نفس الوقت فى قتل روح الابتكار.

**ب- إن حماية برامج المعلوماتية تحول دون القرصنة الدولية للبرامج[2]:**

لا شك أن عدم شمول برامج المعلوماتية بالحماية، سيفضى إلى تفاقم مشكلة القرصنة الدولية لهذه البرامج، وارتكاب كافة الجرائم المعلوماتية التى تدخل فيها الاعتداء على البرامج، لاسيما وأن هذه الجرائم تتسم بصعوبة الكشف عنها وصعوبة إثباتها وذلك لتميز مرتكبى هذه الجرائم بمهارات ومعارف فنية خاصة، ولأن مرتكبيها يرغبون فى المال فضلاً عن قهر النظام[3] وهى أمور تبين إلى أى مدى يتعين على ا لدول أن تتعاون، لإشاعة البرامج المبتكرة التى تخدم الإنسانية فى مقابل مبالغ معقولة، بدلا من انصراف الأفراد والدول إلى القرصنة.

ولقد دلت الإحصاءات الحديثة على أن القرصنة فى بعض الدول قد بلغت حجما يهدد أنظمة المعلومات فى العالم، فنصف البرامج فى الولايات المتحدة تقلد وفى كندا وصلت النسبة إلى تسعين فى المائة، وهذا يكلف اقتصاد هذه الدول

---

(١) المرجع السابق – ص ٣٤. وانظر كذلك:

- Francois. Wallon. Le Prix d'un programme. Expertires No. AV. 1981, p.15.

(٢) محمد محمد شتا – فكرة الحماية الجنائية لبرامج الحاسب الآلى – دار الجامعة الجديدة – سنة ٢٠٠١ – ص ٢٢.

(٣) العقيد/ علاء محمد شحاته، «جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات»، بحث قدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، سالف الإشارة، ص ١١ ود. زكى زكى أمين حسونه، «جرائم الكمبيوتر... بحث قدم لنفس المؤتمر، ص ٩.

مئات ملايين الدولارات، ويقول رأى أن الشعور بخطر عمليات القرصنة أخذ فى التزايد بعد الاستخدام العالمى لشبكات محلية ودولية، فى معالجة البيانات والمعلومات عن بعد نظير أجر نقدى(١)، فالاستيلاء غير المشروع على المعلومات يهدد المبتكرين أفراداً وأشخاصاً معنويين بخسائر فادحة، وبالإفلاس على نحو يستلزم شمول البرامج بشتى أنواع الحماية الجنائية من الناحيتين الموضوعية والإجرائية، بغية الحيلولة دون سيادة القرصنة الدولية للبرامج، ذلك أن الجرائم المتصلة بنظم المعالجة الآلية للمعلومات هى جرائم عالمية، ولهذا فإن اهتماماً دولياً بمكافحة هذه الجرائم قد بدأ يتضح فى الآونة الأخيرة على المستويين العالمى والإقليمى(٢).

**ثالثاً: أهمية الحماية المعلوماتية: في تحقيق أهداف التنمية الاقتصادية:**

**تلعب برامج المعلوماتية دوراً رئيسياً في تحقيق التنمية الاقتصادية، لذا فإن حماية البرنامج تعد حماية لأهداف التنمية في حد ذاتها:**

١- وبياناً لذلك فإن البرنامج الذى يصاغ لبيان كيفية إنتاج سلعة استراتيجية، مثل السلع التى تنتج عن صناعة الحديد والصلب، ومراحل الإنتاج، والضوابط التى بمقتضاها يتميز هذا الإنتاج هو برنامج هام، فإذا تم الوصول إليه وإفادة دولة أخرى منه، فإن تلك الدولة الأخرى تستطيع أن تنتج هذه السلعة دون أن تتكبد مشاق البحوث وتكاليفها، ومن ثم تستطيع أن تغرق أسواق العالم بسلعة رخيصة نتيجة اعتدائها على برنامج المعلوماتية الخاصة بدولة بذلت جهوداً ولم تجن ثمارها(٣).

---

(١) د/ محمد حسام لطفى، المرجع السابق، ص ٣٥، والمراجع التى أشار إليها.

(٢) د/ عمر الفاروق، جرائم الكمبيوتر، بحث مقدم لمؤتمر المشار إليه سابقاً، ص ٩، وهامش ١.

(3) See for exemple: Lotus Development carporation: LOTUS NEWS 1991, PP. 60-150.

مشار إليه لدى: محمد محمدشتا - المرجع السابق - ص ٢٣.

وهكذا فإن حماية البرامج فى مثل هذه الحالة هو حماية لأهداف التنمية الاقتصادية ذاتها.

٢- كذلك قد يوجد برنامج يحدد كيفية إنتاج نوع من الأصواف خفيف الوزن وغير قابل للكرمشة، نتيجة خلط خامته بمواد أخرى تزيده متانة ولا تقلل من طبيعته، هو برنامج هام فى نقل البلاد نقلة حضارية هائلة، تمكنها من إنتاج سلعة تستطيع بموجبها ليس فقط أن تنافس منتجى الأصواف فى المجال الدولى بل أكثر من هذا أن تسبقهم وتوسع المسافة بينها كدولة مقدمة وبينهم، فإذا تم الاعتداء على هذا البرنامج فإن التنمية الاقتصادية فى دولة تصنيف هذا البرنامج تتأثر لا محالة لنفس الاعتبارات السابقة، طالما لم يتم تطوير البرنامج، إذ التطوير يولد المشروعية(١).

٣- كما أن هناك من البرامج ما يقدم ابتكارات جديدة فى مجال استخدام الطاقة الشمسية، والرياح فى توليد الكهرباء فى الصحراء والإفادة منها فى تحلية مياه البحر، ومن ثم إقامة مجتمعات عمرانية جديدة على الشواطئ بما يقلل من الكثافة السكانية داخل البلاد، ويفتح المجال أمام فئة جديدة من أبناء البلاد فى إنتاج سلع جديدة، والقيام بأعمال لم يكونوا يطرقونها من قبل، مثل صناعة صيد الأسماك وتعليبها أو صناعة السياحة، وما إلى ذلك، فإذا تم الاعتداء على البرنامج الذى يبلور هذه المسائل وأمثالها فإن ذلك يضر بالمصالح الاقتصادية للدولة، التى بذلك أبناؤها جهوداً كبيرة فى سبيل إنجاز هذا البرنامج للنهوض باقتصادها وتمنيتها(٢).

٤- وإذا كان وقود التنمية وأساس استمرارها هو رأس المال، فإن برامج

---

(١) أنظر: د/ أسامه محمد محيى الدين عوض، نداء إلى علماء القانون الجنائى، بحث قدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى سالف الإشارة، ص ١٣.

(٢) أنظر فى بيان يتعلق بتسجيل الجرائم الاقتصادية الذائعة: د/ هشام محمد فريد رستم، قانون العقوبات ومخاطر تقنية للمعلومات، (أسيوط: مكتبة الآلات الحديثة، ١٩٩٤م)، ص ٢٠٧ وما بعدها.

المعلوماتية قد تنطوى على أفكار تقلل من تكاليف الإنتاج، بأن تختصر مرحلة مكلفة من مراحله، أو تستعيض بالميكنة (الآلية) بدلاً من العنصر البشرى فى أداء مهام يصعب على الإنسان أداءها، أو تستخدم سلعة وسيطة أقل تكلفة وأكثر متانة، فإذا صيغ كل ذلك فى قالب برنامج معلوماتى، فإنه يؤدى لا محالة إلى توفير المال للقيام بعملية التنمية الاقتصادية خير قيام، ومثل هذا البرنامج يجب حمايته حتى يتحقق للدولة التى صنف أبناؤها البرنامج فائض فى الميزانية المالية تمكنهم من الاستمرار فى إبداعهم وإلا فإن اقتصاد الدولة سينهار إذا تمكنت دولة أخرى أو شركات أخرى من الحصول على البرنامج وتنفيذه.

٥- ولعل ذلك بين أسباب اتجاه بعض الأفراد والدول للغش المعلوماتى فى قطاعات تساهم فى تحقيق التنمية، مساهمة فعالة مثل البنوك، وغيرها وتشير بعض المجلات العلمية المتخصصة، إلى أن ١٩ ٪ من حالات الاعتداء على برامج المعلوماتية المتمثلة فى أفعال الغش المعلوماتى تستهدف البنوك و ١٠ ٪ منها تستهدف الإنتاج الصناعى[١]، ومن هنا فإن السوق الشرعى للمعلومات Marche légal l' de l' information قد تقلص لحساب سوق سوداء Marché noire ترتبط «بالجزء الأعظم للأنشطة الاقتصادية للمجتمع»[٢].

إن حماية برامج ونظم المعلومات يفضى لا محالة إلى تحقيق أهداف التنمية الاقتصادية، فى الدول التى يبتكر أبناؤها هذه البرامج التى تساعد على تحقيق التنمية الاقتصادية[٣].

---

(١) د/ محمد سامى الشوا، «الغش المعلوماتى كظاهرة إجرامية مستحدثة»، بحث قدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى، سالف الإشارة، ص ١٦.

(٢) المرجع السابق.

(٣) محمد محمد شتا - المرجع السابق - ص ٢.

## المطلب الأول

## الوسائل القانونية لحماية المعلوماتية

نتيجة للتطور التكنولوجى التقنى للمعلوماتية والتقدم السريع والمتواصل الذى تخطوه أغلب الدول لتطوير الأجهزة والبرامج المعلوماتية، وإعتماد قطاعات عديدة من المجتمعات على التقنية المعلوماتية على المستوى الدولى والمستوى الوطنى فى شتى المجالات والميادين الاقتصادية والسياسية والثقافية والاجتماعية، فقد أفرز ذلك إتساع فى دوائر إستخدام الحاسبات الالكترونية والنظم المعلوماتية خلال القرن الماضى بإضطراد وتطور غير مسبوق ومستمر وبسرعة فائقة، وأصبحت معظم الأجهزة العامة والخاصة تعتمد على الحواسب فى تسيير شئونها، وتقليص دور الأوعية الورقية، وإقتران ذلك بالاعتماد على أوعية مادية أخرى – غير ورقية – فى البيئة المعلوماتية كالملفات والأشرطة والإسطوانات والأقراص الممغنطة.

وأزاء هذا التغيير المصاحب للتقدم التكنولوجى المعلوماتى، أصبح لزاماً على الدولة – ممثلة فى كيانها التشريعى – أن تبسط حمايتها على هذا الكيان الجديد، وتوفر له سبل تأمينية ووسائل قانونية تتفق وطبيعته.

وتبرز المشكلة فى بسط الحماية القانونية على النظام المعلوماتى، إلى تلك السمات التى تميز هذا الصنف من الجرائم التى تستهدف البيئة المعلوماتية، والتى تصل بنا إلى حقيقة صعوبة اكتشاف الجريمة المعلوماتية، حيث أنها جريمة هادئة لا تتسم بالعنف(*)، وهى جريمة فنية لا يتخلف عنها أثار مادية

(*) ربما كان السبب فى صعوبة بسط الحماية القانونية المطلوبة، هو أن الجرائم المعلوماتية لا تترك أثر يدل عليها بذاتها، كآثار العنف التى يتركها الاعتداء على الاشخاص والأشياء المادية، لأنها تتعامل مع بيانات وأرقام ومعلومات مخزنة الكترونياً، ورغم ذلك فإن البعض يشبه هذه الجرائم بجرائم العنف، حيث ذهب مكتب التحقيقات الفيدرالى بالولايات المتحدة الأمريكية (FBI) إلى أن جرائم الحاسب الآلى Computer Crimes هى بمثابة جرائم عنف Asvi-olent crimes، وهذا التشبيه لا يعتمد على الآثار وإنما يعتمد على الدوافع. إذ يرى

=/=

ملموسة، كتلك التى تخلفها جريمة السرقة أو جريمة الاعتداء على الأخرين، كما وأنها جريمة ترتع فى البيئة الرقمية وتنتقل بين البيانات، من حيث التغيير أو المحو من الذاكرة، أو الأضافة للمحتوى.

ولاشك أنه كلما تقدم الإنسان فى فهم تكتيك العمل فى الأنظمة المعلوماتية، كلما استطاع أن يرتكب جريمته دون أن يخلف آثار يمكن الاهتداء إليه من خلالها، ولهذا تعتبر الجريمة المعلوماتية من أهم الجرائم التى تحتاج إلى حماية جنائية كافية، وهو أمر توصل إليه القضاء الفرنسى فى أحكام عديدة أصدرها[1].

وباستعراض موقف القضاء الفرنسى نذهب إلى أن الحماية الجنائية للبيانات المعالجة الكترونياً، يجب أن تكون أبعد مدى وأكثر تنظيماً وتخطيطاً بشكل يفوق مجرد توقعات الأحكام القضائية، حيث أن محل الجريمة المعلوماتية لا يتمثل فى المكونات المادية للأنظمة المعلوماتية، كسرقة الأجهزة والمعدات ذاتها، وإنما يتعلق الأمر بالنظم المعلوماتية ذاتها، والفكر الابتكارى الذى نسق ونظم هذه النظم[*].

---

اصحاب هذا الاتجاه أن دافع المتلصصون والمعتدون والدخلاء على النظام المعلوماتى، إنما هى دوافع متماثلة مع دوافع مرتكبى العنف من مشعلى الحرائق أو مفجرى المفرقعات.

- Computer Hackers: tomorrows Torrorists, Dynamics, News for and about members of the American Society for industrial security, January & February 1990, p. 7.

(1) Voir Par exemple Arrété du 22 décembre, 1981, Cité dans gl thése de M. pouger Francois la Protection des Logiciel (Paris II) non empr. p. 20.

مشار إليه لدى: محمد محمد شتا – المرجع السابق – هامش ١ – ص ٩٧.

(*) ذهب الفقه فى هذا الشأن إلى أن النظم المعلوماتية تحمل فى ثناياها إمكانية غير مسبوقة للنفاذ والتسلل إلى دخائل الفرد وأسراره، ومن ثم الاعتداء على حقه فى الحياة الخاصة من خلال المعلومات المخزنة عنه فى بنوك المعلومات أو فى حاسبات جهات معينة. (المرجع السابق – ص ١٠١).

والبادى في الموضوع أن النصوص الجنائية التقليدية التى تكفل الحماية القانونية للحق فى الخصوصية، كالنصوص التى تحمى حرمة المساكن (المواد ١٢٨، ٣٦٩، ٣٧٠ عقوبات)، والحياة الخاصة والمحادثات (م ٣٠٩ مكرر عقوبات)، وأسرار المهنة (م ٣١٠ عقوبات)، لا تكفى لكفالة هذه الحماية فى مواجهة خطر الإجرام المعلوماتى.

**أولاً: دور المشرع في مواجهة المد الإجرامي المعلوماتي:**

إنه إذا كان مقبولا من القضاء أن يواجه هذه الصعوبات بتفسير للنصوص الجنائية يوسع من نطاق تطبيقها، بما لا يجاوز المدى الذى يمكن أن تمتد إليه عباراتها، فكذلك يكون مقبولاً ومتطلباً منه دائماً التمسك بمبدأ الشرعية الجنائية، وما يتفرع عنه من حظر القياس فى مواد التجريم والعقاب، وأن يمارس المشرع مسئولياته فى تجريم ما يستجد من الأفعال الضارة بالمصالح الجوهرية للمجتمع(١).

وعلى المشرع أن يحرص على الوقوف على مدى كفاية النصوص التجريمة التقليدية فى التشريعات القائمة، لمواجهة ما تثيره تقنية المعلومات من مشكلات، وتقصى مدى ومواضع الحاجة إلى معالجة هذه المشكلات، بنصوص جنائية مستحدثة تلائم الطبيعة غير المادية لبعض عناصر ومكونات أنظمة الحاسبات، والطابع التقنى الخاص بأساليب ارتكاب الجريمة فى بيئة المعالجة الآلية للبيانات، وصولاً إلى تقرير مدى كفاية وفاعلية الحماية التى يبسطها قانون العقوبات على البيانات المعالجة اليكترونيا بوجه عام، والاجتهاد فى تعزيز فاعلية هذه الحماية وتلافى ما قد يعتريها من نقص(٢).

وقد تبدو هذه الموضوعات صعبة التنفيذ، لا سيما مع صعوبة اكتشاف هذه الجرائم، وتبدو الصعوبة أكثر وضوحاً، اذا تعلق الأمر ببيانات هامة مثل:

---

(١) المرجع ذاته.

(٢) د/ هشالم رستم - مرجع سابق - ص ٢٢١.

- **بيانات ذات صلة بالذمة المالية:**

كاستيلاء غير مشروع على البيانات المعالجة الكترونياً، وهى تتم من خلال عدة صور:

أ – الاستيلاء على البرامج والبيانات المعالجة الكترونيا، دون أن يقترن ذلك باختلاس أوعيتها المادية(*) .

ب– النسخ غير المشروع للبيانات المخزنة الكترونياً، وهذا أيضاً لا يترك أى اثر(**) .

جـ– الالتقاط الهوائى للبيانات المعالجة أو المنقولة الكترونياً(١) .

ولا شك أن عدم ترك هذه الجرائم أثاراً يلقى تبعة شديدة على النيابة العامة أثناء مباشرتها التحقيق فى أحداها، ويصبح لزاماً عليها أن تستعين بالخبراء المختصين فى هذا المجال من ذوى الخبرة العملية والقدرة الفكرية العالية، ليتثنى مواجهة هذا الإجرام التقنى، والقضاء على الظواهر الإجرامية الخطيرة فى نطاق المعلوماتية، من خلال إجراءات قانونية واعية تتفق ومعطيات العصر، ونصوص عقابية حازمة تطبق للردع وأقرار القانون ونصرة العدالة .

**ثانياً: الاجتهادات القانونية لتحقيق الأمن المعلوماتي:**

إن النصوص القانونية المبتغاه لحماية النظم المعلوماتية هى السبيل الأهم، لمعالجة القصور التشريعى الواضح حالياً، والقاصر عن المواجهة الفعالة الرادعة أمام النشاط الإجرامى المنتهك لنظم أمن المعلومات .

---

(*) كما فى الألتقاط الذهنى Captation-Intellectuelle للبيانات، يراها الإنسان ويحفظها ولا يترك ذلك أى أثر.

(**) لأن البيانات المعالجة الكترونياً تخزن على هيئة نبضات كهربائية فى دوائر إلكترونية مجمعة، أو تخزن على أشرطة أو اسطوانات ممغنطة، فيقوم الجانى بنسخها على دعامات أخرى دون أن يترك ذلك أثراً. إلا إذا تم اتخاذ إجراءات دفاعية صارمة على الاستنساخ.

(١) المصدر ذاته.

وهكذا فقد تفشت جرائم الغش المعلوماتي وأصابة المعطيات والبرامج والكيانات المنطقية المختزنة فى الحاسب الآلى، وكثرت الأنشطة الإجرامية فى الحصول بطريق الغش على الخدمات التى يقدمها الحاسب، أو فى استخدام بطاقات الأنتمان – الدفع الإلكترونى – سواء الصحيحة أو المنتهية أو المزورة فى سحب مبالغ مالية غير مستحقة تصيب الانتمان البنكى أصابات بالغة، أو فى اقتحام نظام المعالجة الآلية للمعلومات بطريق الاحتيال أو النصب. أو فى تخريب المعلوماتية والمعطيات والبرامج، أو فى إتلاف المعلومات أو تعطيلها أو تعديلها وإلغاء البعض منها أو معظمها، أو تزوير أنظمة المعلومات ومعطياتها والبرامج المنفذة من خلالها.

جميع هذه الجرائم – نتاج ما أفرزته التقنيات الحديثة – المستحدثه، دفعت الفقه إلى الاجتهاد بأقتراح نصوص عقابية[1]، بغيت فرض سياج قانونى يوفر نواحى أمنية أكثر فاعلية للمعلوماتية، نعرض لهذه المواد فى صياغتها المقترحة[2]، علّ أن تكون نموذج يسترشد بها المشرع فى خطواته المحمودة لمواجهة الجريمة المعلوماتية.

**المادة الأولي:**

يعاقب بالحبس والغرامة التى تصل إلى عشرة أضعاف قيمة المعلومات والبرامج، كل من حصل بطريق الغش على برامج مختزنة فى الحاسب الآلى أو النظام أو التى تظهر على شاشة الحاسب أو المسجلة على اسطوانات أو شرائط ممغنطة أو غيرها، أو حصل عليها أثناء نقلها، أو استخدم أو نسخ هذه المعلومات، أو اعطاها للغير من أجل نسخها أو لأى غرض آخر.

(١) د/ جميل عبد الباقى الصغير – جرائم الكمبيوتر والجرائم الأخرى فى مجال تكنولوجيا المعلومات – بحث مقدم للمؤتمر السادس للجمعية المصرية للقانون الجنائى – القاهرة – الفترة من ٢٥:٢٨ أكتوبر ١٩٩٣ – ص ص ١٢، ١٣.

(٢) أعاد صياغة هذه المواد الباحث/ محمد محمد شتا – فكرة الحماية الجنائية – مرجع سابق – ص ٢٧ وما بعدها. آخذاً فى الإعتبار نصوص الحماية المقررة فى قانون حماية حق المؤلف واتفاقية تربس (TRIPS).

المادة الثاني:

يعاقب بالحبس مدة لا تزيد على خمسة أعوام، أو بعقوبة الجريمة المقترفة أيهما أشد، كل من حصل بطريق الغش على الخدمات التى يقدمها الحاسب الآلى أو استعمل هذا الحاسب بقصد ارتكاب جريمة.

وتكون العقوبة السجن أو العقوبة المنصوص عليها للجريمة، أيهما أشد إذا استخدم الحاسب فى ارتكاب جريمة من الجرائم المضرة بأمن الدولة.

المادة الثالثة:

يعاقب بالحبس وبغرامة تعادل ضعف المبلغ الذى حصل عليه، أو بأحدى هاتين العقوبتين كل من استخدم بطاقة الإئتمان الخاصة به سواء كانت صحيحة أو ملغاة، فى سحب مبالغ – من خلال أجهزة التوزيع الآلى للنقود – تتجاوز رصيده فى البنك أو تتعدى المبلغ الذى يضمنه هذا الأخير.

المادة الرابعة:

يعاقب بالحبس وبغرامة لا تقل عن عشرة آلاف جنيه كل من اقتحم بطريق مشروع نظام المعالجة الآلية للمعلومات. فإذا نجم عن هذا الفعل تعطيل تشغيل النظام أو المحو أو تعديل فى المعطيات المخزنة فيه تكون العقوبة الحبس الذى لا تقل مدته عن ستة أشهر، والغرامة التى تعادل ضعف الضرر الذى ترتب على فعله.

المادة الخامسة:

يعاقب بالحبس وبغرامة تعادل ضعف الضرر المترتب على الفعل كل من خرب أو أتلف عمداً المعطيات أو المعلومات أو البرامج أو الكيانات المنطقية التى لا يمتلكها أو جعلها غير صالحة للاستعمال أو عطلها بأية طريقة. وتكون العقوبة السجن إذا كانت المعلومات أو المعطيات تتعلق بأمن الدولة أو بأية مصلحة قومية أخرى.

المادة السادسة:

يعاقب بالحبس وبغرامة تعادل ضعف الفائدة التى حصل عليها أو الضرر الذى ترتب على فعله كل من عدل أو أضاف أو ألغى كل أو بعض المعلومات أو البرامج أو الكيانات المنطقية الخاصة بنظام المعالجة الآلية للمعلومات من أجل الحصول على فائدة له أو غيره، أو بقصد إلحاق الضرر بأصحابها.

المادة السابعة:

كل من زور فى المعلومات أو المعطيات المختزنة فى النظام أو المسجلة على اسطوانات أو شرائط ممغنطة أو غيرها من الدعامات، يعاقب بالحبس إذا سبب ذلك ضرراً للغير. وتكون العقوبة السجن إذا كانت المعلومات أو المعطيات تتعلق بأمن الدولة أو بأية مصلحة قومية أخرى، طالما كان يعلم ذلك.

المادة الثامنة:

كل من استعمل عن علم المستندات المزورة الواردة فى المادة السابقة، يعاقب بالحبس بحسب ما إذا كانت المستندات تتعلق بأحد الأشخاص. وتكون العقوبة السجن إذا تعلق ذلك بأمن الدولة، أو بأية مصلحة قومية أخرى(*).

ويمكن للمشرع المصرى الاسترشاد بنهج المشرع الفرنسى فى سبيله لمواجهة الجرائم المعلوماتية، حيث لاحظ الأخير استفحال ظاهرة الإجرام المعلوماتى، فتدخل بسن نصوص جديدة تضمنها قانون العقوبات من شأنها مواجهة هذه الظاهرة، وقد صدر بهذه النصوص قانون ٥ يناير ١٩٨٨، وتم تعديل هذه النصوص جزئياً فى عام ١٩٩٤، كما تم نقلها ضمن أحكام أخرى من قانون العقوبات بعد تعديلة(**).

---

(*) تم تعديل صياغة هذه المادة بمعرفة الباحث، حيث كانت تشمل كلمة الأفراد، فتم استبدالها الأشخاص تشمل الشخص الطبيعى أو المعنوى.

(**) راجع ما سبق فى الدراسة – ص٢٦٨، بشأن تدخل المشرع الفرنسى بسن نصوص عقابية جديدة لمواجهة جرائم التكنولوجيا الحديثة التى تستهدف المعلومات.

جدول يوضح المواد القانونية ذات الصلة بالجرائم المعلوماتية(١)

| التبويب | الموضــوع |
|---|---|
| الجــرائم الماسـة بـأمـن الـدولـة الخارجي: | السعي والتخابر مع دول أجنبية عبر شبكات المعلومات المحلية والدولية. |
| | تخريب وسائل الاتصالات أو مؤسسات حيوية عن طريق إقحام الفايروسات أو البرمجيات التخريبية في النظم البرمجية. |
| | استفادة بمنفعة مادية من دول أخرى للأضرار بمصلحة وطنية عن طريق إحداث خلل فى نظم البيانات وقواعد البيانات. |
| | الحصول بطريقة غير مشروعة على سر من أسرار الدولة الموجودة ضمن قواعد البيانات الوطنية. |
| | إشاعة، او نشر، أي معلومة من المعلومات المحظورة عبر اختراق نظم المعلومات الوطنية. |
| الجــرائم الماسـة بـأمـن الـدولـة الداخلي: | إتلاف بيانات ونظم المعلومات الخاصة بمرافق الدولة، أو المصالح الحكومية. |
| فك الأختـام وسرقة الأوراق: | سرقة أو اختلاس، أو إتلاف ملفات معلوماتية حكومية. |
| | الإهمال فى صيانة أمن المعلومات لأى مستندات حكومية موجودة ضمن نظم المعلومات. |
| الجــرائم المخلة بالثقة العامة: | التقليد الكاذب للملفات ومحتوياتها. |
| الجــرائم ذات الخطر العام: | إتلاف ملفات ووثائق الغير. |
| | تعريض أموال الناس للخطر نتيجة لاختراق معلومات المصارف الحكومية والأهلية وتخريب قواعد بياناتها. |
| | التأثير على سلامة خطوط الملاحة الوطنية بشتى أنواعها عن طريق إقحام فايروسات في نظم إدارة أنشطتها بالحاسوب. |
| | الاعتداء على وسائل الاتصال نتيجة مباشرة اختراقات معلوماتية لسرقة النداءات الهاتفية أو العبث بها. |
| الجــرائم المخلة بالأخلاق والآداب العامة: | التحريض على الفسق والفجور عن طريق إقحام صور أو أفلام مصورة مخلة بالحياء. |
| | العمل الفاضح المخل بالحياء الناجم عن استخدام مواقع الدردشة الإلكترونية، والبريد الإلكتروني. |
| | انتهاك حرمة الغير عن طريق اختراق حواسب الغير عبر شبكة المعلومات المحلية أو الوطنية. |
| الجرائم الواقعة على الأشخاص: | جريمة سرقة ملفات الغير أو جهودهم العلمية المختزنة فى الحواسب الشخصية، أو نظم المعلومات المتاحة فى الشبكات المحلية. |

(١) أ/ حسن مظفر الرزو – الأمن المعلوماتى (معالجة قانونية أولية) – مرجع سابق – ص ٩٢.

## المطلب الثاني

## الوسائل الفنية لحماية المعلوماتية

في إطار بسط سبل الحماية الفنية للمعلوماتية :-

**فقد ذهب رأي فقهي إلي أنه(١)،**

إذا كانت الحكمة تقضى بأن «الوقاية خير من العلاج» (*) فيجب اتخاذ الوسائل الفنية التقنية الكفيلة بمنع ارتكاب الجريمة المعلوماتية، أو على الأقل التقليل من اضرارها، ومن اختراق أنظمة أمن المعلومات، فذلك خير من الانتظار لوقوع الجريمة ثم محاكمة مرتكبيها. ذلك أنه غالباً ما تبوء هذه المحاكمة بالفشل لأسباب عديده منها: عدم كفايه النصوص القانونية المتعلقة بالتجريم والعقاب، أو عدم معرفه الفاعل وعدم كفاية الأدلة، وإما لصعوبة تنفيذ العقوبة، لأن المحكوم عليه يقيم فى الخارج، وعدم كفاية الآليات التقليدية للتعاون القضائى الدولى فى هذا المجال.

وتتمثل الحماية الفنية التقنية فى ايجاد أنظمة أمان لحماية نظم المعلوماتية، وتنقية المعلومات المتداولة عن طريق الشركات المنتجة للبرامج، أو تشفير البيانات بمعرفة أصحاب الشأن.

**أولاً: الوسائل التأمينية:** تتمثل هذه الوسائل فى الزام الشركات المنتجة للبرامج

---

(١) د/ جميل عبد الباقى الصغير – الجوانب الإجرائية للجرائم المتعلقة بالإنترنت – دار النهضة العربية – سنة ٢٠٠١ – ص ١٢.

(*) وعكس ذلك يقول خبراء الكمبيوتر أن مقولة – الوقاية خير من العلاج – لا يمكن تطبيقها بدقة فى مجال جرائم المعلوماتية – جرائم الفضاء الإليكترونى – ومع ذلك فإن من الحماقة أن يترك الفرد منزله غير مغلق عند ذهابه إلى العمل صباحاً، ومن الحماقة كذلك أن يترك – نطاقه المعلوماتى – دون حماية، بحيث يسهل الوصول إليه. يراجع: بيتر إن جرابسكى – الجريمة فى فضاء الإنترنت – بحث ضمن كتاب (الأمن والأنترنت) – من منشورات مركز بحوث ودراسات شرطة دبى – الإمارات العربية المتحدة، ص ٧١، مشار إليه لدى د/ عبد الفتاح بيومى حجازى – مرجع سابق – ص ٢٩٢.

بوضع عراقيل فنية تقنية للحيلولة دون دخول المتلصصون أو القراصنة إلى تلك البرامج وما تحويه بنوك المعلومات وقواعد البيانات والبريد الاليكتروني من اسرار تجارية أو صناعية، أو مراسلات خاصة. وتتمثل هذه الوسائل التأمينية في عدم امكانية الدخول إلى المعلومات إلا باستخدام شفرة Code d'accés معينه أو كلمة سر خاصة Mot de pass (pass word). كما يمكن لهذه الشركات اعداد برامج للشكف عن هوية القراصنة وأماكن دخولهم إلى الشبكة، حيث يكون لهذه البرامج دورها في تخويف من تسول له نفسه محاولة اقتحام الشبكة أو نظام المعلومات. وفي هذا الصدد طالعتنا الصحف المكتوبة(١) بما توصلت إليه إحدى شركات الكمبيوتر التي طرحت للتداول برنامج شهير(*) أطلق عليه اسم «سيندميل»، القادر على تحديد عنوان

---

(١) جريدة الأهرام – الصادرة بتاريخ ١٩ مارس سنة ١٩٩٨ – ص ١.

(*) تحرص الشركات والمؤسسات على الأخذ بأحدث التقنيات في مجال حماية نظم المعلومات، ومن هذه الوسائل:

أ – جدران الحماية: يقوم بدور حارس البوابة بين الإنترنت والإنترنت، وأكثر أنواع هذه البرامج شيوعاً، مرشحات الرزم Packet filters، وجدران الحماية المستخدمة على مستوى التطبيق Application - level firewalls – حيث يقوم مرشح الرزم، وهو يعمل بصورة نمطية على جهاز يسمى السيّر (Router) بفحص عنوان المصدر Source وعنوان الواجهة Desti-nation لكل رزمة من البيانات سواء كانت داخلة إلى شبكة الشركة أم خارجة منها، ويمكن للمرشح منع رزماً آتية من عناوين معينة من الدخول إلى الشبكة، وأن يمنع رزماً أخرى من الخروج منها، أما جدار الحماية المستخدم على مستوى التطبيق، فإنه يقوم بفحص مضمون البيانات المتداولة بالإنترنت اضافة إلى العناوين، لذلك فهو أبطء من مرشح الرزم، ولكنه يسمح للجهة – صاحبة شبكة الحاسب – بتنفيذ خطة أمنية أكثر تفصيلاً.

ب – شهادات توثيق رقمية Digital certificates: وهي طريقة مستخدمة في الإنترنت على نطاق واسع لتبقى وسائل الاتصال مأمونة، فمن أجل ارسال الرسائل وتسلمها بهذه الطريقة، يجب أن يمتلك مستخدم النظام زوجاً من مفاتيح التعمية – التمويه – مفتاح سري خصوصي Private Key، وآخر معلن – عمومي – Public Key، ويتكون كل منهما من سلسلة من البيانات الكثيرة. ويحتفظ المستخدم بالمفتاح السري في مكان أمن، على حين أن المفتاح المعلن يكون معلوماً للأشخاص الذين يرغب في الاتصال بهم.

– ومثال ذلك لو أراد (علي) أن يوجه رسالة إلى (سالم)، ولما كان (علي) يريد أن يكون (سالم)

=/=

المتدخل على شبكة الانترنت، تمهيداً لبث رسائله غير المشروعة عبر البريد الإلكتروني(*).

ثانياً: تنقية المعلومات: توجد طريقتين لتنقية Filtrage المعلومات الجاهزة على

---

== على يقين من أن الرسالة أتية منه فعلاً، فإنه يستخدم مفتاحها السرى، كشهادة توثيق رقمية ترافق رسالته، ويستخدم (سالم) مفتاح (على) المعلن، وذلك للتحقق من توقيعه Signature. لكن كيف يمكن لـ (سالم) أن يتأكد من أن المفتاح المعلن يخص (على) بالفعل؟ وذلك لربما أن يقوم محتال بتزوير كلا المفتاحين الخاصين – بـ (على) ثم ارسال المفتاح المعلن إلى (سالم) مدعياً أنه يخص (على)، وللحيلولة دون ذلك، فإنه يجب على (على) أن يحصل على شهادة توثيق رقمية، وهى وثيقة بيانات تصدرها إحدى هيئات التوثيق المعتمدة على نطاق واسع، أو هيئة توثيق تشكلها الشركة التى يعمل بها المدعو (على).

جـ- صندوق مأمون – للغة البرمجة جافا The Java sandbox: يستخدم المبرمجون لغة البرمجة – جافا – من الإنترنت أو من الشبكات الخاصة بالحواسب الآلية الأخرى، وثمة خطر على هذه الشبكات بأن يقوم شخص غير أمين بتكوين ملحق تطبيق، يمكن أن تكون له القدرة على العبث بنظام الحاسب الآلى وذلك بحذف ملفات أو سرقة بيانات أو تمرير – فيروس – إلا أن لغة البرمجة جافا، قد صممت لتحول دون مثل هذه الانتهاكات. ومفتاح الأمان الخاص ببرنامج جافا، هو من البرمجيات التى تسمى – آلة جافا الافتراضية Java virtual machine وعندما ينسخ مستخدم الإنترنت ملحق لما هو موجود على شبكة الحاسب الآلى، فإن مفتاح جافا يمنع وصول هذا الأمر إلى القرص الصلب فى الحاسب الآلى أو وصلات الشبكة أو الموارد الأخرى للنظام، ولا يمكن استدعاء البيانات من هذا الصندوق، وحسب وسيلة الأمان، إلا فى حالة واحدة هى أن تتحقق – آلة جافا – من أن المستخدم أو البرنامج شخص موثوق فيه، وهذه كلها برامج حماية الهدف منها منع اختراق شبكات الحاسب الآلى.

- راجع فى ذلك د/ رضا عبد الحكيم رضوان – بحث بعنوان – مكافحة جرائم انتهاك الشبكات الحاسوبية – منشور بمجلة الشرطى – دولة الإمارات العربية المتحدة – العدد العاشر – السنة الثالثة عشر – يناير ٢٠٠١.

- ولعل اختراق شبكات المعلومات لما له من خطورة جعل البعض يقول أننا نعيش حرب المعلومات، بوصفها الوجه الجديد للحروب – راجع: هشام سليمان، بحث بعنوان – حرب المعلومات – مجلة الشرطة – وزارة الداخلية – دولة الإمارات العربية – العدد ٣٧١ – السنة ٣١ – نوفمبر ٢٠٠١.

(*) وإن كان هذا البرنامج يمكن أن يثير الجدل حول تعارضه مع حقوق الإنسان، وحرية التعبير عن الرأى.

شبكة الانترنت: التنقية عن طريق مستخدمى الشبكة، وتنقية المواقع، وتفصيل ذلك كما يلى[1]:

١- **تنقية المعلومات بواسطة المستخدم**: توجد برامج تسمح للمستخدم أن يمنع الدخول إلى بعض المواقع[٢]، فالمستخدم يمكنه أن ينشئ لنفسه قائمة بالمواقع المحظور الدخول اليها، كما يمكنه أن يستخدم القائمة التى يقدمها له متعهد البرامج، والذى يقوم بفهرسة أو وضع جدول بعدد كبير من المواقع ذات الطابع الخلاعى. فمثلاً يقدم برنامج Cyberpatrol للمستخدم امكانيه الدخوّل أو عدم الدخول إلى برامج معينه. فهناك ما يتضمن العنف Violence والعرى الجزئى Nudité partielle والعرى الفنى Artistique. وهناك برامج نموذج Standard وضعتها شبكة الويب Web لعمل تصنيف للحاسبات الخادمة بحسب المحتوى، انطلاقاً من معايير متعددة، مثل درجة العنف ودرجة الاثارة الجنسية Degré d'erotisme.... إلخ.

– أما برامج المراقبة Logiciels de contrôle فهى لا تقدم حلاً مرضياً لمشكلة مراقبة المعلومات الجاهزة على شبكة الانترنت، فهى مجرد وسيلة تمكن متعهدى الوصول من اعفاء أنفسهم من المسئولية عن المحتوى غير المشروع للمعلومات والقائها على عائق مستخدمى الشبكة.

كما أن برامج المراقبة يمكن انتاجها فى بلاد لها عادات وثقافات تختلف عن عاداتنا وتقاليدنا، وبالتالى فإنها لا تؤدى الغرض المقصود منها فى حماية القصر من الثقافات الاجنبية، وذلك إلا اذا صمموا برامج خاصة لبلادنا. يضاف إلى ذلك أن الأولاد يعرفون جيداً التكنولوجيا الحديثة، وبالتالى يمكنهم الالتفاف حول رقابة الآباء، ثم أن الآباء قد لا يعرفون هذه التكنولوجيا، الأمر الذى يقلل من دورهم فى المراقبة.

---

(١) د/ جميل عبد الباقى الصغير – المرجع السابق – ص ١٣.

(2) TOURNIER (Jerôme), Internet censure à domicile. Le Monde supplément multimédia, 19 Février 1996, p. 28.

٢- **تنقية المواقع:** يجب أن نعلم أن تنقية المواقع هو أمر صعب جداً ويمكن التحايل عليه بطريقة أو بأخرى بواسطة مستخدمى الشبكة(١)، مع ملاحظة أن تنقية المواقع يمكن أن تتم على مستوى العناوين أو على مستوى الخدمات.

ولأهمية تكنيك التنقية اقر مجلس الشيوخ الامريكى قانون يعاقب على التوزيع – عن طريق المواقع التجارية على شبكة الانترنت – للمواد الإباحية Matériel pornographique للقصر، كما يلزم المكتبات التى تحصل على اعانات بأن تدخل برامج فلترة Logiciels de filtrage (٢).

كما قضت المحاكم الأمريكية(٣)، بمسئولية شركة Prodigy لأنها قدمت نفسها للجمهور على أنها تمارس رقابة على محتوى الخدمات التى تتولى تقديمها باستخدام برامج تنقيه Filtrage من نوعية خاصة، وباتباع منهج معين يقوم به أشخاص متخصصين فى هذا المجال، ومع ذلك لم تقم بمنع الرسائل والمعلومات غير المشروعة، وبالتالى تكون قد أخلت بالتزامها بتنقية المعلومات على الشبكة.

**ثالثاً: أشهر برامج حماية أمن المعلوماتية:** أثمرت الجهود الدولية عن ايجاد العديد من الإجراءات الحمائية، منها ما هو على مستوى الفرد ومنها ما هو على مستوى المؤسسات المالية الكبرى ومنها أيضاً ما هو على المستوى الدولى.

---

(1) SÉDALLIAN (V.), Droit de l'Internet, Réglementation. responsabilités. Contrats, Collection AUI, Paris 1996, p. 136.

(2) LOUNDY (David J.) et BELL (Blake A.), droit du cyberespace#1, disponible à l'adresse: http:// www. juriscom. net/droit/elaw/e-law/1/ htm. p.8; http:// www. digiplace.come/e-law/cyberdroit.htm; p.8: http:// www. nyti mes.com/library/tech/98/07/cyber/articles/22 filter-html.

(3) THOUMYRE (Lionel), Responsabilités sur le web: une histoire de la réglementation des réseaux numériques, disponible à l'adresse: http: // www. lex-electronica.org/articles/v6-1/thoumyre.htm, N°, 35, p. 7.

أ - فعلي مستوي الفرد: قامت الشركات المنتجة للبرمجيات بانتاج العديد من البرامج التى يمكن استخدامها لحماية نظم المعلومات المخزنة بالحاسب، من هجمات فيروسات الحاسب الآلى المختلفة.

ومن أشهر تلك البرامج(١):

- برنامج Trojan AID NIT - 4.5، وهو برنامج لمقاومة الفيروسات من نوع تروجان.
- برنامج Surfin Guard، ويعمل هذا البرنامج لحماية الحاسب من الملفات المحملة بالفيروسات التى قد تنتقل إلى الجهاز من خلال شبكة الانترنت، ويقوم هذا البرنامج بتخصيص منطقة آمنه على الحاسب تسمى "Samdbox" حيث يقوم بفحص الملفات المطلوبة من شبكة الانترنت قبل فتحها.
- برنامج "PC - Cillin"، وهو برنامج خاص بحماية الجهاز من آية فيروسات قد يتعرض لها، أثناء التعامل اليومى مع البريد الاليكترونى.

ب- علي مستوي الكيانات الاقتصادية:

أما على مستوى البنوك والمؤسسات المالية، فقد اتجهت غالبيتها خاصة الدولية منها – إلى تبنى واعداد البنية التحتية لنظم تشفير الرسائل والمعاملات عبر شبكة الانترنت المعروفة بـ PKI أو الـ Personal Key Infrastractues مثل نظام SET أو ما يعنى العمليات الإليكترونية المؤمنة Secure electronic Trans-actions ونظام الـ 3 Domain Secure.

وفى نطاق البنوك فقد قامت العديد منها فى الدول الغربية بتطبيق برنامج الشبكة العصبية أو Neoro Net، وهو أحد برامج الكومبيوتر الذى يمكنه مراقبة كافة التعاملات، التى تتم باستخدام البطاقات الخاصة بالبنك سواء كانت ممغنطة أو ذكية، واكتشاف العمليات المشبوهة اليكترونياً فى مهدها.

---

(١) جمال عبد المنعم محمد وآخرون – مرجع سابق – ص ٧٨.

وفى مجالات التجارية الإليكترونية أيضاً - قامت بنوك أخرى بتطبيق برنامج حماية لتمييز العمليات التى تتم عبر شبكة الانترنت عن غيرها من العمليات، والزام المشترى بضرورة أن يكون العنوان الذى سيتم شحن السلعة المشتراه إليه، هو ذاته عنوان صاحب البطاقة المستخدمة المدون لدى البنك المصدر لها.

وفى هذا المجال أيضاً فأنه تجدر الاشارة إلى امكانية الاستفادة من نظام تأمينى، متاح لكل مستخدمى أجهزة الحاسب الآلى، يوفره برنامج التصفح عبر شبكة الانترنت المسمى بـ نتسكيب Netscape - ويسمى هذا النظام بـ SSL ويتم استخدامه حالياً بمعرفة العديد من البنوك والمؤسسات المالية والأفراد.

**جـ- من أحدث وسائل حماية الأمن المعلوماتي(١):**

**(١) برنامج Down 2000 Lock:**

ومن محاسن هذا البرنامج أنه قوى وشامل للحماية الفردية إلا أن عيوبه إطلاق صفارة التخزين فى كل تغيير يحدث بملف.

**(٢) برنامج Yammer:**

يتم من خلال مراقبة تامة لكافة المنافذ فى وقت واحد، ومن الجوانب الفنية لاستخدامه:

أ - إدخال كلمة السر عند كل بداية لتشغيل الجهاز.

ب- يقوم هذا البرنامج بالحماية من المخترقين، حيث أنه يراقب المنافذ لمراقبة أى حركة دخول أو خروج للبيانات، ويعطى تنبيه صوتى مع رسالة موجزة عند محاولة أى شخص الدخول إلى الجهاز.

جـ- إغلاق الثغرات الأمنية التى عادة تترك مفتوحة، حيث يغلقها البرنامج بطريقة آلية ودون تدخل من المستخدم.

---

(١) حسن مدحت الروبى وآخرون - مرجع سابق - ص ٣٩ وما بعدها.

د - يتحسس الجهاز وجود ملفات التجسس بداخله، حيث يقوم بازالتها آلياً ولديه القدرة على اكتشاف برامج التجسس وإلغائها.

هـ- يوفر ثلاث مستويات للحماية الأولية، عند التشغيل فقط والحماية الثانوية عند التشغيل، بالإضافة لبعض وسائل الحماية الضرورية الأخرى.

و - الحماية الشاملة، حيث لا يمكن تشغيل أى برنامج من البرامج المخزنة بالجهاز.

**(٣) برنامج Alert 99 Internet:**

وهو برنامج سهل وبسيط وتشغيلة قوى فى حمايته من المحترفين المخترقين، إلاّ أن عيبيه السماح للآخرين بالدخول باذن من المستخدم أو غيره، إن كان الجهاز يستخدمه أكثر من مستخدم، وهو من البرامج القوية ويؤدى الحماية على ثلاثة محاور رئيسية هى:

أ - المراقبة الشاملة للمنافذ.

ب- إعطاء تنبيه صوتى عند محاولة الدخول، وتسجيل رقم المخترق والوقت والتاريخ.

جـ- يوضح موقع المخترق من خلال خريطة عالمية تشمل جميع شركات الاتصالات بالعالم، ويزود المستخدم باسم مزود الخدمة التى سجل معها المخترق ورقم التليفون والبريد الالكترونى.

**وهناك العديد من البرامج والأساليب الأخري للحماية منها:**

١- ضد الفيروسات ويكون لحماية الحواسب من الشبكات والرسائل الالكترونية والملفات، التى يتم تحميلها من شبكة الانترنت أو أى مستخدم داخل الشبكة الداخلية، وتنقية المعلومات الشبكية من أى موقع فيه بحث عن البرامج الغير مرغوب فيها، وبرنامج لإيقاف البرمجيات الضارة التى قد تنتقل للجهاز، أثناء التجول على الانترنت والشبكات.

٢- النقل والتحميل الدورى للملفات الموجودة بالهارد ديسك على وحدات تخزين منفصلة، تتفادى حدوث أى عطل يؤدى إلى فقدان هذه المعلومات، وكل هذه الإجراءات تكون منظومة متكاملة وشديدة الترابط فيما بينها، هدفها النهائى هو التأمين الشامل لنظم المعلومات ضد الجريمة المعلوماتية.

٣- من خلال أخطار شرعية على المستخدم، وهو برنامج يستخدم فى تحديد الصلاحيات المتاحة للمستخذمين للشبكة الداخلية أو شبكة الانترنت من حيث الاتصال والحصول على المعلومات والتعامل معها، مع إضفاء الشرعية التوثيقية لهذه الصلاحيات.

٤- نظم تأمين شبكات الحاسب ذات الطابع التكيفى ومنها: البحث الأمنى لإظهار نقاط الضعف التى يمكن من خلالها الاختراق، إلى أى حاسب شخصى أو حاسب مركزى سواء من داخل الشبكة الداخلية أو خارجها، ولضمان التأمين ضد أى محاولة يتم الاستعانة ببرنامج الكشف عن أى اختراق، وهذا البرنامج يعمل طوال ٢٤ ساعة ومن أهم حزم البرامج للتأمين:

أ - البحث على مستوى الشبكات.

ب- البحث على مستوى قواعد البيانات العلاقية.

جـ- لكشف محاولة اختراق الشبكات.

د - لكشف محاولة اختراق أنظمة التشغيل.

**د - الجدار الناري Fire Wall:**

أغلب خبراء المعلوماتية ذهبوا إلى أن الجدار النارى(*): هو برنامج يمكن أن يكون على هيئة جهاز متكامل أو برنامج يتم تحميله إلى الحاسب الآلى بمواصفات جيدة. وظيفته حماية شبكة الحاسب الآلى الداخلية وشبكة الانترنت،

---

(*) **حائط النيران:** نظام أمن لحماية شبكات المنظمات ضد المقتحمين والمخربين، فهو يمنع الأجهزة المستخدمة للشبكة من الاتصال مباشرة مع حواسب خارج الشبكة، بل توجه كافة الأتصالات الخارجية من خلال برامج مختلفة أو أجهزة مختلفة الطراز، فإنه يلزم التحويل من هيئة لأخرى. (مهندس/ على يوسف على - مرجع سابق - ص ٢٨٩).

ووظيفته الرئيسية مراقبة كل البيانات الداخلية والخارجية من الشبكة،والتأكد من مطابقتها لشروط المستخدم التى يحددها للبرنامج من قبل.

وتختلف أنواع الجدران النارية فقد يكون الجدار النارى برنامجاً أو جهازاً، ومهما اختلف أشكالها ومع تعدد الشركات الصناعية، فإنها جميعها تعمل بنفس الفكرة والتقنية، وتقريباً تتساوى فى قدراتها فى حماية الشبكة، ولكن الاختلاف يكون فى طريقة تركيبها وبرمجيتها(*).

---

(*) توجد برامج عديدة لجدران النار من ذلك: برنامج شبكة (DAN)، والذى يتضمن مزايا أمنية عديدة عبارة عن برامج جدران النار Fire Walls، ومزودات بروكسى Proxy Servers التى تحتفظ بصفحات الشبكة – للويب – على القرص الصلب، ومرشحات عناوين arl filters.

– وتشبه برامج جدران النار حرس الحدود على الساحل، حيث تزود الشبكات بحماية جيدة عن طريق التأكد من شرعية كل شخص يود زيارة الشبكة المحمية دخولاً أو خروجاً دون أن يكون مصرحاً له بذلك.

– وتشبه – مزودات بروكسى – الشاحنات العسكرية الخاصة بالتموين، والتى تجلب البضائع، وهى فى هذه الحالة صفحات الشبكة الخارجية، حيث يعاد توزيعها داخلياً، وتساعد عملية التوزيع الداخلى على خفض حركة المرور عبر بوابة الدخول إلى الشبكة المحلية، لأنها تلغى الحاجة إلى استدعاء البيانات مرة ثانية من مواقعها على شبكة إنترنت، إذ سبق استدعائها وحفظها على القرص الصلب فى الشبكة المحلية، وتستخدم مزودات بروكسى – كذلك – لمنع دخول البيانات الوافدة من إنترنت إلى الحاسب الآلى بالشبكة المحلية، بصفة جزئية أو كلية.

– أما مرشحات (URL) فهى ببساطة عبارة عن – فلتر يمنع مستخدمى الشبكة من الدخول إلى مواقع معينة على شبكة الإنترنت، وبالتالى تعطى صاحب الشبكة أو مالكها الحق فى التحكم فى مستخدمى الشبكة أن يدخلوا أم لا إلى مواقع معينة غير مرغوب فيها على الشبكة.

– ولعل هذه الميزة من الأهمية بمكان فيما يتعلق بتصفح الطفل أو الحدث للإنترنت بطريقة آمنة، بحيث لا يتسلل إلى المواقع الإباحية أو تلك التى يحصل منها على خبرات ضارة.

– ويتم إستخدام برمجيات – جدار النار – عند الأماكن التى تتلاقى فيها الشبكة الداخلية للشركة أو المؤسسة، مع شبكة إنترنت العالمية، ويمكن القول – بصفة عامة – أنه كلما زاد عدد خدمات الإنترنت التى يسمح بها لمستخدمى الشبكة فى المؤسسة المحلية، تزداد الخطورة من الدخول إلى شبكة إنترنت العالمية، ولذلك تأتى وظيفة جدران النار فى هذه الحالة، ويكون هدفها حماية المناطق الهامة من الشبكة الداخلية للمؤسسة الخاصة أو العامة – راجع فى ذلك، تقريراً بعنوان «حصن شبكتك الداخلية من عدوان إنترنت»، منشور فى مجلة إنترنت العالم العربى، عام ١٩٩٨، على موقع: http:// www. ditnet.co.ae.

مشار إليه لدى: د/ عبد الفتاح بيومى حجازى – مرجع سابق – ص ٢٩٣.

إلا أنه عندما يقرر المرء تركيب جدار نارى فى شبكته الداخلية، يجب معرفة أن إسناد هذه المهمة بالجدار لا يفيد فى شئ إن لم يتم تركيبه بالشكل المناسب، مثل الحارس الذى يتم وضعه أمام باب ولم يحدد مهامه، فلن يمنع أحد من الدخول إن لم يطلب منه ذلك.

والجدار النارى ضرورى جداً لكل شبكات الحاسب الآلى فى أية مؤسسة إذا ما تقرر الارتباط بالانترنت وإلاّ فالعواقب وخيمة.

رابعاً: التشفير Codage (Cryptographie)[(١)]، هو عملية تتمثل فى تحويل المعلومات المقروءه إلى اشارات غير مفهومةInintelligibles[(٢)]. فبعض مستخدمى شبكة الانترنت يبتغون أن يتمكنوا – بواسطة برنامج خاص – من تشفير معلوماتهم قبل نقلها عبر الشبكة، على أن يتم فك رموزها ببرنامج مماثل عند استقبالها من جانب المرسل إليه. فالتشفير هو وسيلة لحماية أمن المعلومات ضد اعمال القرصنة، وبث الفيروسات والاعتداء على المعلومات الأسمية، وبيانات بطاقات الائتمان الممغنطة[(*)].

ولذلك اتفقت شركتا ماستر كارد وفيزا كارد على تقنيات فنية مشتركة (التشفير)، لحماية التسويق الذى يتم عبر شبكة الانترنت باستعمال بطاقات الائتمان Credit Cards.

---

(١) د/ جميل عبد الباقى الصغير – الجوانب الإجرائية المتعلقة بجرائم الانترنت – مرجع سابق – ص ١٥ وما بعدها.

(2) GOLIARD (F.), Télécommunication et réglementation française du cryptage, D. 1988, Chron., p. 120

(*) ويلاحظ أنه لا يمكن إجراء عملية التشفير فى فرنسا إلا بعد الحصول على ترخيص بذلك من الوزير المختص، وعدم الحصول على هذا الترخيص يشكل جنحة، كما يعاقب تحت وصف المخالفة كل من قام بالامداد بوسائل التشفير أو قام بتصديرها.

- VERGUCHT (Pascal), La répression des délits informatiques dans une perspective internationale. Thèse, Montpellier I, 1996, N°, 315, p. 390.

وتستخدم برامج الـ S.S.P أو «طبقة الادخال الأمنية» Secure socket payer لتشفير الطلبات وتخزينها على المزود فى منطقة خاصة لا يستطيع سوى مدير الموقع (أو من يفوضه) الوصول إليها، وبالتالى يمكن حماية المعلومات الخاصة بالبطاقات الائتمانية من الاستخدامات غير المشروعة(*).

ومع ذلك فللتشفير خطورته، حيث أنه يجعل مهمة البوليس مستحيلة، لأنه يمنعه من اكتشاف الجرائم التى تتضمنها الحاسبات الآلية، وخاصة بالنسبة للإرهابيين ومروجى الصور ذات الطابع الإباحي، الأمر الذى يشكل أيضاً عقبة تحول دون اتمام التحقيق الابتدائى(١).

فنظام التشفير يجعل إقامة الدليل على ارتكاب الجريمة أمراً مستحيلاً. وهذا ما حدث فى قضية السيد/ Faurisson (٢)، حيث نشرت رسائل عنصرية ومضادة لليهودية Révisionniste تحمل اسم Robert Faurisson وتم اكتشافها على أحد المواقع بعنوان Aaargh، والذى تم ايواءه فى أمريكا. إلا أن المحكمة لم تستطع اقامة الدليل على أن هذا المتهم هو صاحب الرسالة المجرمة. وأضافت المحكمة أن وجود اسم المتهم فى نهاية المقال لا يعنى أنه قد صدر عنه، على أساس أن هذا الاسم يمكن لأى شخص أن يكتبه إمعاناً فى التمويه، الأمر الذى يقتضى

---

(*) وتعمد وسيلة التشفير إلى تحويل كل طرف أو رقم داخل الملف المراد تشفيره إلى كود مقابل له، وذلك عند الإرسال وعندما يقوم المستخدم المسموح له بقراءة الملف باستقباله، فأنه يستخدم مفتاحاً معيناً لقراءته، يطلق عليه أسم (مفتاح فك الشفرة).
للمزيد يراجع: على يوسف على – مرجع سابق – ص ١٧٤، حرف C.

(1) BERTHOU (renaud), Internet et le respect des principes essentiels du droit du for, disponible à l'adresse: http:// www.juriscom. net/ Universite/memoire 12/presentation.htm. p.3.

(2) T.G.I., 13 Novembre 1998, disponble à l'adresse: http:// www. legal-is.net/jnet/decisions/illicite - divers/corres - paris - 1998 - htm.

الزام متعهد الوصول بتحديد شخصية المشترك وعدم توصيل الأسماء المجهوله بشبكة الانترنت(١).

ولخطورة تقنية التشفير سنت بعض الدول - مثل هولندا - مشروع قانون يخضع عملية التشفير للحصول على ترخيص Autorisation مع الالتزام بإيداع مفاتيح الشفرات Dépôt des clés des codes لدى مكتب متخصص ملتزم بالسرية، والذى يجب عليه أن يقدم هذه المفاتيح لرجال البحث الجنائي الذين

---

(1) JOUGLEUX (Philippe), La criminalité dans le cyberespace, Mémoire de D.E.A. Droit des médias, Aix - Marseille, 1999, pp. 183 et 184; BERTHOU (Renaud), Internet et le respect des principes essentiels du droit du For, op. cit., p. 86.

وانظر فى ذات الموضوع:

- leymonerie (Romain), Cryptage et droit d'auteur, disponible à L'adresse: http:// www. juriscom. net/universite/memoire3, presentation, htm, 1996.

- ونظراً لأن عمليات التشفير تجعل من إقامة الدليل على ارتكاب الجريمة أمراً مستحيلاً، لذا اتجهت العديد من دول العالم إلى حظر عمليات التشفير المعقدة أو وضعها تحت السيطرة الحكومية أو القضائية، لضمان مراقبة العمليات المشبوهة التى تتم عبر تلك الشبكة.

لمزيد من المعلومات فى هذا المجال يمكن مراجعة موقع http://www.inscure.orgl كما يمكن مراجعة موقع المباحث الفيدرالية الأمريكية على شبكة الانترنت بالمكلف بالتحقيق فى الاختراقات غير القانونية لشبكات الحاسب فى الولايات المتحدة على العنوان: http://www. Ibi.gov/programs/ipcis/index.

- ويشار فى هذا الصدد إلى وجود نظام اليكترونى يستخدم لمراقبة واعتراض خطوط الاتصالات الاليكترونية التى تجرى في جميع انحاء العالم، وعملية مراقبة الاتصالات الاليكترونية تقوم حالياً باختبار أكثر من ٣ بلايين اتصال يومى وتشمل المكالمات التليفونية ورسائل البريد الاليكترونى والفاكسات والإرسال المنبعث من أى قمر صناعى بالفضاء وعمليات انزال الملفات من على شبكة الانترنت، ويتم هذا المشروع بالتعاون بين عدة دول منها الولايات المتحدة وانجلترا واستراليا وكندا ونيوزيلاندا - والاسم الكودى للمنظمة المسئولة عن تلك العمليات هو Echelon وتعنى القفل. حيث تستخدم تطبيقات حديثة تعتمد على نظم الذكاء الاصطناعى لفلترة البيانات والحصول على المعلومات المهمة والمفيدة. (يراجع: جمال عبد المنعم محمد وآخرون - مرجع سابق - ص ٨٠).

حصلوا على أمر بالضبط والتفتيش من سلطات التحقيق، وإن كان احتمال افشاء مثل هذه المفاتيح قد يضعف من وسائل الحماية ضد الجرائم المعلوماتية(١).

ولأن المشرع الفرنسى قدر أن استخدام التشفير فى نقل المعلومات قد يسهل الأنشطة الإجرامية، فإنه تدخل ونظم هذه العملية بنصوص قانونية(٢).

وفى الولايات المتحدة الأمريكية طعن أحد الاساتذة بجامعة Western بعدم دستورية القانون الذى يحظر تصدير برامج التشفير L'exportation des logiciels d'encryptage والتكنولوجيا المتعلقة بها. إلا أن المحكمة رفضت دعواه، على أساس أن التشفير ليس عقبة أمام ممارسة حرية التشفير التى نص عليها الدستور(٣).

إلا أن وسائل الحماية الفنية التقنية لا تكفى وحدها لحماية شبكة الانترنت والمعلومات التى تمر بها من مخاطر الاختراق أو التجسس عليها، الأمر الذى يدعونا إلى بحث مدى امكانية اضفاء هذه الحماية عن طريق القضاء المستجل(٤).

**خامساً: الاستفادة من الـ HACKERS في نظم أمن المعلومات:**

– ورغم خطورة المخترقين والهاكرز واستغلالهم عمليات الاختراق فى السطو على أموال البنوك، وسرقة أرقام بطاقات الائتمان، فقد ظهر اتجاه معاكس لمواجهتهم يتمثل فى سعى الشركات الكبرى إلى خطب ودهم وكسب ثقتهم(*).

---

(1) VERGUCHT (P.), La répression, op. cit., N°, 315, p. 391.

(٢) القانون رقم ٩٦ – ٦٩٩ الصادر فى ٢٦ يوليو سنة ١٩٩٦ بشأن تنظيم الاتصالات عن بعد: Jo. du 27 Juillet 1996.

(3) LOUNDY (D.J), et BELL (B.A.), op. cit., p. 17, le jugement est accessible à l'adresse suivante: http://samsara. law.cwru.edu/comp - law/jvd et http:// jya.com/pdjl 1.html.

(٤) د/ جميل عبد الباقى الصغير – مرجع سابق – ص ١٧.

(*) ولقد تنبهت الشركات الكبرى العاملة فى مجال تقنية المعلومات إلى ما يمكن أن يضيفه الهكرة فى مجال الأمن المعلوماتى، وبدأت فى البحث عنهم ومنحهم فرص عمل حقيقية لتسخير قدراتهم الأمنية والمعلوماتية، للعمل بأسلوب قانونى والاستفادة منهم فى كشف الثغرات الأمنية

–/–

وقد انتشرت فى أوساط مواقع الانترنت فى عقد التسعينات – من القرن الماضى – العديد من المنظمات التى ترعى الـ Hackers أو القرصنة، سعى بعضها إلى الدفاع عن المفهوم الحقيقى لهذه الجماعات الذى يتمثل فى إلغاء الحدود أمام عمليات سبر أغوار الحواسب والشبكات، وابتكار طرق جديدة للتعامل مع أجزائها الدقيقة، والتوجه نحو التثقيف المعلوماتى(1)، بينما حملت منظمات أخرى أهدافاً تخريبية يروجها الـ Hackers مثل بث البرامج الخبيثة ونشر طرق الاعتداء على الخصوصيات المعلوماتية، واختراق شبكات المعلوماتية(*).

– والأكثر من ذلك أن بعض الحكومات قد تجد فى التعامل معهم، مكاسب ينبغى ألا تفوت فرصة الحصول عليها، وذلك بالنظر إلى المصالح الأمنية لهذه الحكومات(2).

---

= فى البرامج والنظم التى تنتجها هذه الشركات وثغرات برامج الشركات المنافسة كذلك. ويرغب الكثير من الهكرة الذين لا يسعون إلى مخالفة القانون فى العمل فى مثل هذه الشركات، الأمر الذى يسمح لهم بممارسة هواياتهم دون أن يخالفوا القانون، ويتعرضون للملاحقة القانونية، ولذلك تحرص الكثير من الشركات المنتجة لمضادات الفيروسات، والشركات العاملة فى مجال أمن الشبكات والمعلومات على حضور مؤتمرات الهاكر، والبحث عن الخامات المؤهلة للعمل فى شركاتهم، وتتغاضى الشركات عن ماضى هؤلاء والذى يحتمل أن يكون تخريبياً أو اجرامياً لأن ما يهمهم هو القدرات العلمية التى يمكن أن تفيد الشركة – راجع ما سبق – منظمات الهاكر وتجمعاتهم – على موقع .http:// www. dit net. co. ae

(1) اللواء/ نجاح محمد فوزى – وعى المواطن العربى تجاه جرائم الاحتيال – مرجع سابق – ص40.

(*) كثيراً ما تلجأ الجهات الحكومية فى العديد من الدول إلى التعاون مع تلك المنظمات فى سبيل التوصل إلى كسر – حل – شفرة معينة أو اختراق شبكة أو موقع معين للتوصل إلى جهات تخالف القانون، بل إن الأمور قد وصلت إلى ما هو أبعد من ذلك، حيث تقوم بعضٌ من تلك المنظمات بتنظيم مؤتمرات عالمية يجتمع فيها كل من الـ Hackers والمسئوليون عن الأمن المعلوماتى، وبعض عملاء أجهزة المخابرات الحكومية للعديد من الدول فى قاعة واحدة بهدف تبادل المعلومات والخبرات فى أحدث ما توصل إليه العلم من تقنيات حديثة فى مجال الأمن المعلوماتى.

(2) تتغاضى الكثير من دول العالم عن الهكرة، لأنهم يشكلون أكثر العاملين فى المجال الأمنى من تقنية المعلومات ابداعاً، على أمل أن يؤدى ذلك إلى ظهور ابتكارات جديدة، وأن يشكل هؤلاء

–/–

## المطلب الثالث

## الوسائل الدولية لحماية المعلوماتية

إذا كان التعاون الدولى هو السبيل الفعال لمكافحة جرائم المعلوماتية فإن هذا التعاون يقتضى التخفيف من غلو الفوارق بين الأنظمة العقابية الداخلية ، لأن التباعد بين هذه الأنظمة يجعل المجرم المعلوماتى يبحث عن الأنظمة القانونية الأكثر تسامحًا . ولذلك أبرمت العديد من الاتفاقيات الدولية فى مجال التعاون الدولى ، تستهدف التقريب بين القوانين الجنائية الوطنية من أجل مكافحة الجرائم عابرة الحدود . وتظهر معالم هذا التقارب فى قبول حالات تفويض الاختصاص فى اتخاذ اجراءات التحقيق وجمع الأدلة وتسليم المجرمين والاعتراف بالأحكام الجنائية الأجنبية . وهذا التعاون القانونى الدولى لا ينل من سيادة الدولة ، بل على العكس فإن انعدام هذا التعاون يزيد من التباعد بين الأنظمة العقابية، ممايساعد على تزايد الجرائم عابرة الحدود ومنها جرائم المعلوماتية (١) .

---

-- الهكرة أرضاً خصبة، لظهور تقنيات متطورة، ذلك أن الهكر بمعناه الحقيقى هو الابتكار التقنى والمعلوماتى، والقفز فوق جميع العوائق التى تحد من مدى الابداع، ومنها العوائق القانونية.

– ويمكن القول أن عدم تضنييق النطاق على الهكرة فى أنحاء كثيرة من العالم سبب رئيسى فى ارتفاع مستوى الأمان فى الشبكات، وابتكار أساليب تبادل آمن للمعلومات عبر الإنترنت، ذلك أن السماح لهم بممارسة أنشطتهم أدى إلى كشف الكثير من الثغرات الأمنية والبرمجية، وظهرت نتيجة لذلك، ابتكارات وأساليب حديثة فى التشفير، وفى نقل البيانات، تغلبت على هذه الثغرات، ولولاها لاحتاج العاملون فى مجال تقنية المعلومات على الأغلب إلى سنوات طويلة أخرى، للوصول إلى المستوى الذى نحن عليه اليوم.

– ويمكن تشبيه أثر الهكرة على تقنيات المعلومات، بالتأثير الذى تركته الحرب العالمية الثانية على مختلف العلوم، حيث أدت إلى قفزات نوعية فى عديد منها على الرغم من الأضرار الجسيمة التى تسببت بها، ويجب الاعتراف بأن هؤلاء الهكرة ساهموا بشكل أو بآخر فى تقدم الكثير من الأساليب المعلوماتية الحديثة، وفى رفع مستوى الأمان الذى وصلت إليه البرمجيات وأنظمة الشبكات المستخدمة حالياً، راجع – منظمات الهاكر وتجمعاتهم – مرجع سابق – على موقع http:// www. dit net. co.ae.

(١) د/ جميل عبد الباقى الصغير – مرجع سابق – ص٧٤ .

مبررات التعاون الدولي : يجد التعاون الدولي في مكافحة الجريمة – بصفة عامة – تبريره في بعض الاعتبارات ومنها : –

١- أنه يعتبر خطوة على طريق تدويل القانون الجنائي . ذلك أن ثمة قواعد موضوعية واجرائية تهيمن على أذهان العديد من مشرعي القرن العشرين ، ومن شأن تشابه هذه القواعد أن يخلق نوعًا من التقارب بين التشريعات الحالية ، يجعل الحديث عن توحيد أو تدويل القانون الجنائي أمراً قابلاً للتحقيق (١). وبذلك نقف على أعتاب قانون جنائي دولي في سبيل مكافحة الجريمة المنظمة عابرة الحدود .

٢- أنه يعتبر من قبيل التدابير المانعة من ارتكاب الجريمة ، لأن المجرم سوف يجد نفسه محاطاً بسياج مانعة من الافلات من المسئولية عن الجريمة التي ارتكبها ، أو من العقوبة التي حكم عليه بها . فإذا ارتكب جريمته في دولة ما وتمكن من الهروب إلى دولة أخرى ، فإنه سوف يكون عرضة للقبض عليه أو ترحيله إلى البلد الآخر . ومن شأن كل ذلك أن يجعل المجرم يعزف عن سلوك سبيل الجريمة (٢). بما يحقق الردع الخاص للمجرم المعلوماتي، وعلى المستوى الأعم يتحقق الردع العام عندما تجد العقوبة سبيلها للتطبيق على الجريمة المعلوماتية المرتكبة .

والتعاون أو التنسيق بين التشريعات المختلفة من أجل مكافحة جرائم المعلوماتية يقتضي من كل دولة أن تقوم بتطبيق قوانينها على ما يرتكب فوق اقليمها من جرائم ، وذلك بالنسبة للأفعال التي تتفق التشريعات المختلفة على العقاب عليها . فمثلاً دعارة الأطفال Pédophilie هو أمر مستهجن عالمياً ، فإذا قامت كل دولة بمحاكمة الجناة الذين يقومون ببث صور دعارة الأطفال التي

---

(١) د/ حسنين عبيد – التعاون الدولي في مكافحة الجريمة ، مجلة القانون والاقتصاد – س٥٣ – سنة ١٩٨٣– ص٢٥٧ .

(٢) المرجع السابق – ص٢٥٨ .

ترتكب على اقليمها باستخدام الانترنت Servant de l'internet ، فإن ذلك سوف يساهم فى تقليل هذه الظاهرة الاجرامية ، إن لم يؤد إلى القضاء عليها . ففى انجلترا مثلاً صدرت عدة أحكام بالادانة بعقوبة الحبس ضد أشخاص قاموا ببث صور تتعلق بدعارة الأطفال على شبكة الإنترنت (١).

وللتعاون الدولى صور عديدة يهمنا منها فى مجال مواجهة الجريمة المعلوماتية، التعاون القضائى، وتسليم المجرمين .

## الفرع الأول

## التعاون القضائى

يعد التعاون الأمنى الدولى والمساعدة القضائية فى قضايا المعلومات، من أهم صور التعاون الدولى القضائى فى مجال الجرائم عابرة الحدود ، ومنها جرائم المعلوماتية وانتهاك أمن المعلومات .

**أولاً : التعاون الأمنى الدولى :** إن مكافحة أساليب الاجرام المعلوماتى لا يتحقق إلا إذا كان هناك تعاون دولى على المستوى الاجرائى الجنائى (٢)، بحيث يسمح بالاتصال المباشر بين أجهزة الشرطة فى الدول المختلفة ، وذلك عن طريق انشاء مكاتب متخصصة لجمع المعلومات عن مرتكبى الجرائم المعلوماتية وتعميمها (٣) .

فأنه يصعب على الدولة بمفردها القضاء على جرائم المعلوماتية عابرة الحدود، لأن جهاز الشرطة فى هذه الدولة أو تلك يصعب عليه تعقب المجرمين ومتابعتهم إذا ما عبروا حدود الدولة . ولذلك فإن الحاجة ملحة إلى تعاون أجهزة الشرطة بين الدول وتنسيق العمل فيما بينها لضبط المجرمين، ومكافحة نشاط

---

(1) YAMAN AKDENIZ, Pornography on The Internet : http : // www. argfia.fr/lij/english/ArticleJuinII.html, 1996 .

(2) MERLE (R.) et VITU (A.,) Problèmes généraux, op. cit., T. 1, N° 325, pp. 432 et 424 .

(٣) د/ جميل عبد الباقى الصغير – مرجع سابق – ص ٧٥ .

الإجرام المعلوماتى التى يتجاوز حدود الدولة . وقد تبلور هذا النوع من التعاون الدولى فى إنشاء المنظمة الدولية للشرطة الجنائية (الانتربول Interpol)(*).

وتستهدف هذه المنظمة تأكيد وتشجيع التعاون بين سلطات البوليس فى الدول الأطراف ، على نحو فعال يحقق مكافحة الجريمة ، وذلك بتجميع البيانات والمعلومات المتعلقة بالمجرم والجريمة من خلال المكاتب المركزية الوطنية للشرطة الدولية الموجودة فى أقاليم الدول المنضمة، وتبادل المعلومات والبيانات فيما بينها ، والتعاون فى ضبط المجرمين بمساعدة أجهزة الشرطة فى الدول الأطراف ومدها بالمعلومات المتوفرة لديها على اقليمها . أى أن عضو الانتربول لا يقوم بنفسه باجراء القبض على المجرم ، بل أن هذا العمل منوط بجهاز الشرطة الوطنية فى الدولة التى يتواجد المجرم على اقليمها (١) ، الأمر الذى يؤكد على احترام السيادة الوطنية (٢) .

ولذلك فإنه من الأهمية تدعيم التعاون بين أجهزة الشرطة فى الدول المختلفة بناء على اتفاقيات دولية . ولهذا التعاون أهميته بحيث إذا اكتشفت الشرطة الوطنية لدولة ما أن أحد جرائم المعلوماتية قد تم ممارستها عبر شبكة الإنترنت من خلال موقع موجود فى الخارج ، فإنها تقوم بالابلاغ عن هذه الجريمة إلى سلطات البوليس بالدولة التى تم منها البث (**) .

كما يجب أن تعين كل دولة الإدارة الأمنية المكلفة بمكافحة هذا النوع من النشاط الإجرامى ، فيوكل إليها تلقى البلاغات التى محورها جريمة معلوماتية،

---

(*) انشئ هذا الجهاز سنة ١٩٢٣ تحت اسم اللجنة الدولية للبوليس الجنائى Comission internationale de police criminelle والذى تغير إلى مسمى المنظمة الدولية للبوليس الجنائى Organisation internationale de police criminelle سنة ١٩٥٦ . وتضم هذه المنظمة ١٦٠ دولة كأعضاء فيها . يراجع :

- VERGUCHT (P.), op. cit., N° 227, p. 417.

(1) Ibid.

(٢) د/ جميل عبد الباقى الصغير – المرجع السابق – ص٧٦ .

(**) وذلك مثل جرائم بث صور إباحية أو الاعلان عن مواقع جنسية ، أو ممارسة النصب والاحتيال المعلوماتى ، أو القيام بأعمال القرصنة المعلوماتية .

ويكون من اختصاصها إتخاذ الاجراءات القانونية المناسبة - حسب القوانين الوطنية - وتنفيذ التدابير الأمنية الواقية، من استفحال هذا الخطر الملاصق للتقنية الحديثة، والهادم للاستفادة الصحيحة من المعلوماتية (*).

إلا أن مشكلة وضع الضوابط القانونية التى تحكم نظم مرور المعلومات عبر شبكة الإنترنت تثير اختلاف واسع المجال فى المجتمعات الغربية ، يصل إلى حد الجدل وإفساد العرض لجوانب المشكلة ، حيث أضحت شبكة المعلومات (الإنترنت) تستخدم فيها بشكل عادى شمل جميع أنشطة الحياة بمختلف مظاهرها اقتصادية وتجارية واجتماعية وترفيهية، مع اختلاف الثقافات.

---

(*) فى مصر تتولى الإدارة العامة للمعلومات والتوثيق مهام مكافحة الجريمة المعلوماتية وذلك من خلالها اداراتها الفنية المتخصصة ، ومجموعات من العاملين المتخصصين والفنيين ذوى الكفاءة التقنية العالية (ضباط - وموظفون) ، وصلت بهم الخبرة الفنية المعلوماتية درجات عالية فى متابعة الجرائم المعلوماتية عابرة الحدود بين الدول .

كما تساهم إدارة مكافحة جرائم التزييف والتزوير التابعة للإدارة العامة لمباحث الأموال العامة بقدر كبير فى مكافحة جرائم النصب والاحتيال المعلوماتى ، وجرائم سرقة المال المعلوماتى ، بما تضمه من وحدات للبحوث الفنية متكاملة التجهيزات تقدم الدعم الفنى والتقنى لضباط الإدارة فى سبيل قيامهم بمهام المكافحة .

وفى الصين وسنغافورة رغم اتصالهما بشبكة المعلومات (الإنترنت) ،إلا أنهما وضعا رقابة شديدة على المعلومات التى يسمح لمواطنيها بالدخول إليها . ومن أجل تحقيق هذا الهدف تلزم الصين مستخدمى شبكة الإنترنت بتسجيل بياناتهم لدى مكاتب الشرطة . يراجع :

- SEDALLIAN (V.) Droit de L'internet, Op. Cit., p. 140 .

كما أنشأت .U.S.A نقطة مراقبة على شبكة المعلومات تحت مسمى (شرطة الإنترنت Web Police ) ، لتلقى شكاوى مستخدمى الشبكة ، وملاحقة الجناة والقراصنة الكترونياً والبحث عن الأدلة ضدهم وتقديمهم للمحاكمة . (مجلة زهرة الخليج - س٢٠ - العدد ١٠٢٨ - الصادرة بتاريخ ٥ ديسمبر ١٩٩٨ - ص٥٢) .

- وهذا أمر طبيعى ، لأن استخدام الإنترنت على نطاق واسع فى تبادل المعلومات وفى المعاملات المالية والتحويلات المصرفية ، وما يتطلبه ذلك من الحفاظ على سرية البيانات والمعلومات الشخصية ، يقتضى انشاء شعبة بوليس للإنترنت تلحق بالانتربول الدولى Interpol ، لملاحقة الانتهاكات والجرائم التى تستخدم فيها شبكة الشبكات . فبوليس الإنترنت هو نوع من الاجراءات والضمانات للمحافظة على أموال الغير وأسرارهم .

فالبعض يرى ضرورة وضع قواعد بحيث لا تؤدى إلى المساس بالحريات العامة فى تبادل المعلومات وحقوق الاتصال من ناحية ، وألا تستخدم الشبكة لأغراض اجرامية أو نشر مواد إباحية تسئ للمجتمع من ناحية أخرى (١) .

ورغم ذلك ، فإن مهمة أجهزة الأمن فى متابعة الجرائم المعلوماتية تعد مهمة غاية فى الصعوبة – أن لم تكن مستحيلة فى بعض الأحيان – وبخاصة بالنسبة للنشاط الاجرامى الذى يمارس عبر مقاهى الإنترنت Cyber Café (*) .

**- الرقابة علي شبكة المعلومات (الإنترنت) :**

من أجل الرقابة على شبكة الإنترنت طبقت دولة الامارات العربية ما يعرف بنظام الرقيب Proxy الذى يقوم بمراجعة نوعية الخدمات المقدمة عبر شبكة المعلومات (الإنترنت) . فعندما يطلب المشترك موقعاً ما على الشبكة الأم ، تصل الاشارة إلى الرقيب ، الذى يقوم بدوره بعرض الموضوع على قائمة كبيرة جداً من المواقع الممنوعة . فإذا تبين له أن الموقع المطلوب يدخل ضمن هذه القائمة المحظورة فلا يستطيع المشترك الحصول على هذا الموقع ، وتظهر رسالة على الشاشة تقول « تم منع هذا الموقع بواسطة رقيب انترنت الامارات » (٢) .

---

(١) د/ جميل عبد الباقى الصغير – المرجع السابق – ص٧٧ .

(*) هى عبارة عن مكان يضم مجموعة من أجهزة الحاسبات الآلية المرتبطة بشبكة الإنترنت ، ويستطيع الأفراد تأجيرها للدخول إلى شبكة الإنترنت لمدد زمنية مقابل أجر. (مهندس / مصطفى السيد – دليلك الشامل إلى شبكة الإنترنت – دار الكتب العلمية للنشر والتوزيع – القاهرة – سنة ١٩٩٧– ص٢٩ ) .

– فعبر مقاهى الإنترنت Cyber Café يقوم العملاء بتنفيذ ما يعن لهم من جرائم دون إمكانية تحديدهم ، وذلك لأن هذه المقاهى لا تتطلب من عملائها إثبات شخصياتهم . وترتب على ذلك أن المباحث الفيدرالية بأمريكا بعد أن تتبعت أحد القراصنة ، والذى اخترق شبكة معلومات أحد المصارف ، إلا أنها لم تستطع تحديده ومحاكمته ، لأنه تبين أنه نفذ عمليته من خلال عدة مقاهى للإنترنت .

(مجلة زهرة الخليج – س٢٠ – العدد ١٠٢٨ – الصادر فى ٥ ديسمبر سنة ١٩٩٨ – ص٥٢) .

(٢) د/ جميل عبد الباقى الصغير – المرجع السابق – ص٧٨ .

مشيراً إلى القضية رقم ٤٣٧٣ لسنة ١٩٩٧م جنايات أبو ظبى المنظورة أمام قضاء دولة الامارات العربية المتحدة بتاريخ ٢٤/١٢/١٩٩٧م ، وتتعلق بجريمة معلوماتية تم ضبطها بمساهمة مؤسسة الامارات للاتصالات .

وهكذا تتولى المنظمة الدولية للشرطة الجنائية (الانتربول) Interpol اقامة العلاقات بين الدول المنضمة ، وتبادل المعلومات بين سلطات التحقيق فيما يتعلق بجرائم الإنترنت ، وخاصة بالنسبة للجرائم المتشعبة فى عدة دول ، ومنها جرائم الإنترنت .

وعلى نمط الانتربول الدولى ، أنشأ المجلس الأوروبى ، فى لكسمبورج سنة ١٩٩١ بوليس أوروبى L'europol ليكون بمثابة حلقة وصل بين البوليس الوطنى للدول المنضمة من ناحية ، وليستخدم بعد ذلك للملاحقة الجنائية للجرائم عابرة الحدود من ناحية أخرى (١).

**ثانيا : المساعدة القضائية الدولية فى المواد الجنائية :** لما كانت جرائم المعلوماتية ذات طابع عالمى وبالتالى يمكن أن تتعدى آثارها عدة دول، فإن ملاحقة مرتكبى هذه الجرائم وتقديمهم للمحاكمة ، وتوقيع العقاب عليهم ، يستلزم القيام بأعمال إجرائية خارج حدود الدولة حيث ارتكبت الجريمة أو جزء منها ، مثل معاينة مواقع الانترنت فى الخارج ، أو ضبط الأقراص الصلبة التى توجد عليها معلومات غير مشروعة أو صور إباحية ، أو تفتيش الوحدات الطرفية فى حالة الاتصال عن بعد أو القبض على المتهمين ، أو سماع الشهود، أو اللجوء إلى الانابة القضائية، أو تقديم المعلومات التى يمكن أن تساهم فى تحقيق هذه الجرائم . وكل ذلك لا يتحقق بدون مساعدة الدول الأخرى. ولذلك تتضمن معظم الاتفاقيات الخاصة بالجرائم التقليدية نصوصاً، تقضى بضرورة اللجوء إلى المساعدة المتبادلة بهدف تحقيق السرعة والفعالية فى اجراءات ملاحقة وعقاب مرتكبى هذه الجرائم (٢).

ويمكن تعريف المساعدة القضائية الدولية بأنها: « كل اجراء قضائى تقوم به دولة، من شأنه تسهيل مهمة المحاكمة فى دولة أخرى، بصدد جريمة من الجرائم (٣).

---

(1) VERGUCHT (p.), op. cit., N° 227, p. 414.

(٢) د/ جميل عبد الباقى الصغير – المرجع السابق – ص٧٩ .

(٣) سالم محمد سليمان الأوجلى ، أحكام المسئولية الجنائية عن الجرائم الدولية فى التشريعات الوطنية ، (دراسة مقارنة) رسالة دكتوراة – كلية الحقوق – جامعة عين شمس ، سنة ١٩٩٧ ، ص٤٢٥ .

وتتخذ المساعدة القضائية في المجال الجنائي صور عديدة منها [1]:

١- **تبادل المعلومات** : وهو يشمل تقديم المعلومات والوثائق التى تطلبها سلطة قضائية أجنبية بصدد جريمة ما ، عن الاتهامات التى وجهت إلى رعاياها فى الخارج، والاجراءات التى اتخذت ضدهم .

ولا شك أن هذه الصورة من المساعدة القضائية مفيدة للغاية، ونحن بصدد جريمة معلوماتية عابرة للحدود ، حيث أن القوام الأساسى لهذه الجريمة المعلومات عن المتهم المعلوماتى التى قام بتنفيذها .

٢- **نقل الاجراءات** Transmission des procédures répressives : يقصد بنقل الاجراءات قيام دولة بناء على اتفاقية، باتخاذ اجراءات جنائية بصدد جريمة ارتكبت فى اقليم دولة أخرى ولمصلحة هذه الدولة ، وذلك إذا توافرت شروط معينة [2] وهى :

---

(١) د/ جميل عبد الباقى الصغير – المرجع ذاته .
– وهناك مظهر آخر لتبادل المعلومات يتعلق بالسوابق القضائية للجناة Antécédents judiciaires des délinquants من خلالها تتعرف الجهات القضائية بدقة على الماضى الجنائى Passé pénal للفرد المحال إليها ، والتى تساعد فى تشديد العقوبة فى حالة العود ، أو فى وقف تنفيذها . إلا أن تدويل الصحيفة الجنائية Casier judiciaire مازال فى مراحله الأولى ، ففرنسا مثلاً لا تسمح باعطاء صور ضوئية من صحف الحالة الجنائية إلا عن رعايا الدول التى ترتبط بها باتفاقيات تبادل المعلومات .

- MERLE (R.) et VITU (A.), Problémes générau, Traité de droit criminel. procédure pénale, 4 éme éd., Cujas, Paris, 1989, N°326, p. 426 .

مشار إليه فى المرجع السابق ، ص٨٠ .

(٢) د/ سالم محمد سليمان – المرجع السابق – ص٤٢٧ .

(1) VERGUCHT (p.), op. cit., N°332, p. 312.

تتناول العديد من الاتفاقيات الدولية موضوع المساعدة القضائية . مثال ذلك الاتفاق المصرى التونسى الموقع فى ٩ فبراير سنة ١٩٧٦ . فهذا الاتفاق يعتبر تطبيقاً لمبدأ المساعدة القضائية فى المجالات الجنائية والتجارية والمدنية ، وتنظيم قواعد الشهادة والخبرة والمحاكمة وتنفيذ الأحكام بين الدولتين . والاتفاق المصرى الأردنى فى ٢٦ أكتوبر ١٩٨٦ ، والعراقى فى ٦ فبراير ١٩٦٦ ، والكويتى فى ٦ ابريل ١٩٧٧ ، والليبى فى ٢٦ فبراير ١٩٩٢م . يراجع:

–/–

أ- أن يكون الفعل المنسوب إلى الشخص يشكل جريمة فى الدولة الطالبة والدولة المطلوب إليها .

ب- أن تكون الاجراءات المطلوب اتخاذها مقررة فى قانون الدولة المطلوب إليها عن ذات الجريمة .

ج- أن يكون الاجراء المطلوب اتخاذه يؤدى إلى الوصول إلى الحقيقة ، كأن تكون أدلة الجريمة موجودة بالدولة المطلوب إليها .

وقد أقر المجلس الأوروبى اتفاقية نقل الاجراءات الجنائية ، التى تعطى للأطراف المنضمة امكانية محاكمة الجانى طبقاً لقوانينها، بناء على طلب دولة أخرى طرف فى هذه الاتفاقية ، بشرط أن يكون الفعل معاقباً عليه فى الدولتين .

ومع تطبيق هذه الآليات التقليدية (الاتفاقيات) تثار بعض المشاكل ، فمثلاً يثور تساؤل عما إذا كانت اتفاقية التعاون القضائى للمجلس الأوروبى سنة ١٩٥٩

---

-- (د/ عبد الرؤوف مهدى - شرح القواعد العامة للاجراءات الجنائية - دار النهضة العربية - سنة ٢٠٠٠ - هامش ٣١ ص٨٥ ، ٨٦ ) .

وكذلك الاتفاقية الفرنسية المصرية المبرمة فى ١٥ مارس سنة ١٩٨٢ ، وهى تتضمن جملة نصوص تتعلق بالمساعدة القضائية بين الدولتين وتنفيذ الأحكام ، ما لم يكن من شأن هذا التنفيذ أن يمس سيادة احدى الدولتين أو الأمن العام فيها .

(د/ حسنين عبيد - التعاون الدولى فى مجال مكافحة الجريمة - مرجع سابق - ص٢٦٤) .

وفى اطار المجلس الأوروبى أبرمت اتفاقية التعاون القضائى فى المجال الجنائى فى ٢٠ ابريل سنة ١٩٥٩ ، ويمكن تطبيقها على اجراءات المحاكمة التى تتعلق بالجرائم المعلوماتية .

VERGUCHT (p.), op. cit., N°332, p. 411 .

وفى اطار الاتحاد الأوروبى تم اقرار اتفاقية ٢٥ مايو سنة ١٩٨٧ المتعلقة بتطبيق مبدأ عدم جواز محاكمة الشخص عن الفعل الواحد أكثر من مرة ، واتفاقية ١٣ نوفمبر سنة ١٩٩١ بشأن تنفيذ الأحكام الجنائية الأجنبية ، وميثاق ٢٥ مايو ١٩٨٧ بشأن تطبيق اتفاقية المجلس الأوروبى المتعلقة بتسليم الأشخاص المحكوم عليهم ، وميثاق ٢٧ مايو سنة ١٩٨٩ المتعلق بتيسير وتحديث اجراءات تسليم المجرمين .

- Crapport Conseil d' Etat: op. cit., p. 198 .

تطبق أم لا على تفتيش الشبكات المعلوماتية Réseaux informatiques والتصنت Interception على الاتصالات ؟

وفى الواقع، إذا كانت التوصية 10 - R 85 بشأن الانابة القضائية -Commis sion rogatoire كانت تهدف إلى ازالة الشك حول مراقبة الاتصالات عن بعد ، إلا أن لجنة الخبراء المكلفة بصياغة هذه التوصية قد أوضحت فى تقريرها أن هذه الأخيرة (التوصية) لاتطبق على التصنت الذى يتم فى اطار الشبكة المعلوماتية (١) .

يضاف إلى هذه المشاكل التقليدية عقبات أخرى خاصة بالجرائم التى ترتكب فى فضاء شبكة المعلومات (الإنترنت) – وإن كانت توجد على المستوى الوطنى إلا أنها تثار أيضاً على المستوى الدولى – مثل :

١– تتبع الاتصالات الالكترونية عن طريق سلطات التحقيق .

٢– إقامة الدليل على الجرائم التى ترتكب فى مجال المعلوماتية ، وذلك بالنظر إلى الاختلافات التى توجد بين التشريعات المختلفة فيما يتعلق بشروط قبوله الأدلة Admissibilitè des preuves ، وتنفيذ بعض الإجراءات مثل التفتيش عبر الحدود Perquisition Transfrontaliére ، ووقف بث الرسائل ذات المحتوى غير المشروع (٢). ففى كل هذه الفروض يجب أن نعيد النظر فى اطار التعاون القضائى Entraide judiciaire ، من أجل صياغة شكل جديد لهذا التعاون . فمنذ سنة ١٩٩٣ أدرك المجلس الأوروبى المشاكل التى يمكن أن تثيرها التكنولوجيا الجديدة فى مجال الاجراءات الجنائية ، حيث أن

---

(1) Rápport du Conseil d'Etat, Internet et les réseaux numériques, la documenation francaise, Paris, 1998, p. 199 .

(٢) وهذه المشاكل ليست جديدة ، فأنه بإستخدام القمر الصناعى Satelitte والهوائيات Antennes يتلقى مشاهد التلفاز معلومات وصور من جميع أنحاء العالم وهو قابع فى منزله أمام هذا الجهاز.

الاقتراح رقم ١٧ للتوصية رقم R 95 13 قد أكد بوضوح على وجود قصور Lacune على مستوى التعاون الدولي بالنسبة لاجراء التفتيش عبر الحدود (١).

وفى عام ١٩٩٧ أنشأ المجلس الأوروبى لجنة، مهمتها اعداد اتفاقية خاصة لمواجهة الجرائم التى ترتكب فى الفضاء المعلوماتى عبر شبكة الإنترنت (٢).

٣- تبادل الإنابة الدولية القضائية : يقصد بالانابة الدولية القضائية طلب إتخاذ اجراء قضائى من اجراءات الدعوى الجنائية، تتقدم به الدولة الطالبة إلى الدولة المطلوب إليها، لضرورة ذلك للفصل فى مسألة معروضة على السلطة القضائية فى الدولة الطالبة، ويتعذر عليها القيام به بنفسها (٣).

فالانابة القضائية تسهل إذن الاجراءات الجنائية بين الدول ، بما يكفل اجراء التحقيقات اللازمة لتقديم المتهمين للمحاكمة ، والتغلب على عقبة السيادة الاقليمية التى تمنع الدولة الأجنبية من ممارسة بعض الأعمال القضائية داخل أقاليم الدول الأخرى(*).

وتستلزم الأنابة الدولية القضائية ارسال الملف الخاص بالدعوى الجنائية، بمرفقاته – محاضر جمع الاستدلال والتحقيق والمستندات – التى أجريت بمعرفة السلطة القضائية فى الدولة طالبة الانابة، إلى السلطة القضائية فى الدولة المطلوب منها اتخاذ بعض إجراءات التحقيق.

---

(1) Rapport du Conseil d'Etat, Op. Cit., p. 199.

مشار إليه لدى : د. جميل عبد الباقى الصغير – المرجع السابق – ص٨٢ .

(2) Rapport du Conseil d'Etat, Op Cit., p. 200 .

(٣) د/ عبد الرءوف مهدى – شرح القواعد العامة للاجراءات الجنائية (طبقاً لآخر تعديلات) –دار النهضة العربية – سنة ٢٠٠٠ – ص ١٠٢.

(*) مثال ذلك سماع الشهود، وإجراء التفتيش والمعاينات، وكل أعمال التحقيق التى تستدعيها اجراءات السير فى الدعوى الجنائية. وتطبيقاً لذلك قضت محكمة النقض المصرى بأمكانية سماع الشاهد المقيم بالخارج عن طريق الانابة الدولية. (نقض ١٣ أكتوبر سنة ١٩٦٩ – مجموعة أحكام محكمة النقض – ص ٢٠ – رقم ٢١٠ – ص ١٠٦٩).

وقد خلت نصوص التشريع المصرى من أى تنظيم لمسألة الانابة الدولية القضائية، اكتفاء بأحكام تنظيم الانابة القضائية الواردة فى الاتفاقيات الدولية التى انضمت إليها مصر، وبموجب هذه الاتفاقيات فإن الدولة المطلوب منها الانابة تتولى - طبقاً لتشريعها - تنفيذ الانابات القضائية المتعلقة بقضية جنائية(١). ويرسل الطلب من الجهات القضائية فى الدولة الطالبة بالطريق الدبلوماسى(*).

وهذه الاتفاقيات الثنائية Bilatérales أو متعددة الاطراف Multilaterales تتضمن شروط وأساليب تنفيذ الانابة القضائية Commission rogatoire، وغالباً ما تتضمن شرط باستبعاد تنفيذ الأحكام فى المجال السياسى والضريبى أو العسكرى، أو إذا قدرت الدولة المطلوب منها Requis أن التنفيذ المطلوب من شأنه المساس بسيادة الدولة، أو ا لنظام العام أو المصالح الاساسية. الأمر الذى يترك للدولة سلطة تقديرية لتنفيذ أو عدم تنفيذ ما يطلب إليها(٢).

إلا أن مرور إجراءات التعاون القضائى الجنائى الدولى بالطريق الدبلوماسى يجعلها تتسم بالبطئ وكثرة الشكليات Formalistes، وهو ما يتعارض مع طبيعة نظم المعلومات التى تتغير بسرعة عبور وتبادل المعلومة من خلال شبكات الإنترنت، ولذلك تقتضى مكافحة جرائم المعلوماتية ردود سريعة، خشية التلاعب فى البيانات التى يمكن أن تشكل دليلاً ضد المتهم المعلوماتى.

---

(١) د/ عبد الرءوف مهدى - المرجع السابق - رقم ٤٥ - ص ١٠٢.

(*) إلا أن القانون لم يتطلب أن يكون أرسال أوراق الانابة بعد تنفيذها بطريق معين، وان جرى العرف على أن يكون ذلك عن طريق وزارة الخارجية، وفى هذا الشأن قضت محكمة النقض بأنه: ليس فى استلام رئيس النيابة أوراق التحقيق من القاضى العسكرى فى سوريا مباشرة دون وساطة وزارة العدل أو الخارجية مساس بحق من حقوق المتهم، (نقض ١٣ يونيو سنة ١٩٦١ - أحكام النقض - س ١٢ - رقم ١٣١ - ص ٦٧١).

- ومن بين الاتفاقيات التى ابرمت فى مجال الانابة القضائية تلك التى عقدتها فرنسا مع مصر فى ١٥ مارس ١٩٨٢، والاتفاقية المعقودة بين دول الجامعة العربية فى ٩ يونيو ١٩٥٣. (يراجع فى تفصيل هذه الاتفاقيات، حازم مختار البارونى - نطاق تطبيق القاضى الجنائى للقانون الاجنبى - رسالة دكتوراه كلية الحقوق - جامعة القاهرة - سنة ١٩٨٧).

(٢) د/ عبد الرءوف مهدى - المرجع السابق - ص ص ٨٥، ٨٦ - هامش رقم ٣١.

• **الاختصاص القضائي في الجريمة المعلوماتية عابرة الحدود:**

أفادت الطبيعة الدولية لجرائم المعلوماتية تساؤلاً هاماً، يتعلق بتحديد الدولة التى يختص قضاؤها بملاحقة الجريمة[1].

فهل تكون الدولة التى وقع بها النشاط الإجرامى؟

أم الدولة التى توجد بها المعلومات محل الجريمة؟

أم تلك الدولة التى أضيرت مصالحها نتيجة لهذا التلاعب؟

كما أثارت هذه الطبيعة أيضاً، الشكوك حول مدى فاعلية القوانين القائمة فى التعامل مع الجريمة المعلوماتية، وبصفة خاصة فيما يتعلق بجمع وقبول الأدلة المستخلصة من أنظمة الحاسبات الآلية.

**ومن القضايا التي لفتت النظر إلي هذه المشكلات قضية** "R.V. Thompson"[2]:

وتتلخص وقائعها فى قيام مبرمج إنجليزى يعمل بأحد البنوك فى دولة الكويت، بالتلاعب فى نظام الحاسب الآلى الخاص بالبنك ليقوم باجراء خصومات من أرصدة العملاء، ثم يقوم بإيداعها فى الحساب الخاص به. وبعد عودة المتهم إلى انجلترا قام بالكتابة إلى البنك سائلاً إياه أن يقوم بتحويل الحساب الخاص به إلى عدة حسابات بنكية فى إنجلترا، وهو ما قام به البنك بالفعل.

قدم المتهم للمحاكمة بتهمة الحصول على أموال الغير بطرق الاحتيال (المادة ١٥ من القانون الإنجليزى المجرم لفعل السرقة لعام ١٩٦٨)، وحكم عليه بعقوبة السجن. إلا أن المتهم طعن فى الحكم استناداً إلى عدم اختصاص القضاء الإنجليزى بالفصل فى الجريمة، حيث أن فعلى السحب والإيداع قد تما فى دولة الكويت وليس فى انجلترا.

---

(1) Fish Nigri (Deborah), National and International aspects of Computer crime: The Emerging Need for Statutory Controls, Thesis, University of London, 1993, p. 315.

(٢) د/ نائلة فريد قورة – مرجع سابق – ص ٤٩.

وقد رفضت محكمة الاستئناف الطعن المقدم من المتهم، وجاء في حيثيات رفضها بأن النشاط الإجرامي للمتهم لم يكتمل إلا بعد الطلب الذي تقدم به إلى مدير البنك بالتحويل، وما أسفر عنه من حصوله على الأموال محل النشاط الإجرامي بواسطة البنوك الإنجليزية.

وقد لفتت هذه المشكلات النظر إلى ضرورة إيجاد الوسائل المناسبة لتشجيع التعاون الدولي لمواجهة جرائم المعلوماتية، والعمل على التوفيق بين التشريعات الخاصة التي تتناول هذه الجرائم.

حيث يجب أن يشمل هذا التعاون تبادل المعلومات، وتسليم المتهمين، وضمان أن الأدلة التي يتم جمعها في دولة صالحة للاثبات في الاتهام أمام محاكم دولة أخرى، كما أن هذا التعاون يجب أن يمتد إلى مكافحة الجريمة المعلوماتية، وهو ما يقتضي أيضاً تبادل المعلومات بين الدول المختلفة(1).

وتعد الوسيلة المثلى للتعاون الدولي في هذا الخصوص هو إبرام الاتفاقيات الدولية. وتعتبر الاتفاقيات المنظمة لتسليم أو تبادل المجرمين من أهم الوسائل الكفيلة بضمان محاكمة مجرمي المعلوماتية، وتجنب إيجاد ما يسمى بجنة جرائم المعلوماتية "Computer Crime Havens" (*).

إلا أن الوصول إلى ابرام هذه الاتفاقيات يقتضي بطبيعة الحال التنسيق بين التشريعات في الدول المختلفة لضمان تحقق مبدأ ازدواجية التجريم، حيث نجد في جرائم المعلوماتية أن هذا المبدأ يقف عقبه رئيسية، طالما أن كثيراً من القوانين لم

---

(1) Sieber (Ulrich), Criminal Liability for the transfer of Data in International Computer Networks - New Problems for German Law, E.J.C. 1997, Vol. 5, Issue I, p. 114.

(*) وتعني ايجاد منطقة خالية من التطبيق القانوني، يستطيع المجرم المعلوماتي أن يعبث من خلالها بالأنظمة القانونية، ويتحايل على الأحكام العقابية، فيكون من الصعب ضبطه وتطبيق العقوبة المستحقة عليه.

يتم تعديلها بحيث تتواءم مع هذه النوعية من الجرائم، حتى يمكن إدراجها ضمن اتفاقيات تسليم المجرمين.

كما تقوم الاتفاقيات الدولية المنظمة لتبادل المساعدات فى المسائل الجنائية بدور هام فى ملاحقة جرائم المعلوماتية، سواء أكانت بين دولتين أو مجموعة من الدول، حيث يعتمد نجاح التحقيق فى هذه الجرائم بشكل كبير على تبادل المعلومات والأدلة والشهود، والعناية بوسائل الاثبات المختلفة، والتى قد تشترك أكثر من دولة فى اقتسامها فيما يتعلق بالجريمة المعلوماتية الواحدة(١).

ونخلص مما سبق.. إلى أنه فى سبيل مكافحة الجريمة المعلوماتية على المستوى الدولى، يجب أن تتحرك الدول المختلفة – اذا ارادت المواجهة الأمنية السليمة – فى محورين:

**الأول: المحور الأقليمي:**

ويتبدى فى أقدام المُشرع الوطنى على تحديث النصوص العقابية التى تشملها التشريعات الداخلية، بحيث تتواءم مع هذا النمط الجديد من جرائم التقنية الحديثة.

**الثاني: المحور الدولي:**

وسبيله عقد الاتفاقيات الدولية المنظمة لمكافحة الجرائم المعلوماتية، والموضحة للإجراءات المتخذة فى حالة التعددية والاستمرارية للجريمة المعلوماتية، حتى لا يستفيد المجرم المعلوماتى من عجز التشريعات الداخلية عن معاقبته من ناحية، وغياب الاتفاقيات الدولية التى تنظم سبل مواجهته من ناحية أخرى.

- **الوضع علي المستوي الإقليمي:**

تضمن القانون العربى النموذجى بشأن مكافحة جرائم الكمبيوتر والإنترنت فى المادة ٢٢ أنه(٢):

---

(1) Fish Nigri (Deborah), op. cit., pp. 322 - 326.

(٢) د/ عبد الفتاح بيومى حجازى – مبادئ الإجراءات الجنائية (فى جرائم الكمبيوتر والإنترنت) – دار الفكر الجامعى – الإسكندرية – سنة ٢٠٠٦ – ص ٤٩.

«تسرى أحكام التشريع الجنائى للدولة على الجريمة المعلوماتية، إذا ارتكبت كلها أو جزء منها داخل حدودها وفقاً لمبدأ الإقليمية، كما تختص المحاكم فيها بنظر الدعوى المترتبة على تلك الجرائم. وعلى الدول العربية عقد اتفاقيات لتبنى المعيار الأول بالإتباع فى حالة تنازع الاختصاص بين الدول.

كما يسرى التشريع الجنائي للدولة على الجرائم المعلوماتية التى تقع خارج الحدود، إذا كانت مخلة بأمنها وفقاً للقواعد العامة المنصوص عليها فى قانون العقوبات».

وقد تناول هذا النص مسألتى القانون الواجب التطبيق، والمحاكم المختصة بشأن جرائم المعلوماتية، وهذا ما سنعرض له فيما يلى:

**أ - القانون الواجب التطبيق:**

يأخذ المشرع المصرى بمبدأ (الإقليمية)، فيطبق قانون العقوبات على أية جريمة ترتكب داخل القطر المصرى بصرف النظر عن جنسية المتهم أو المجنى عليه فى هذه الجريمة، حيث تنص المادة الأولى من هذا القانون على أنه(*):

«تسرى أحكام هذا القانون على كل من يرتكب فى الأقليم المصرى جريمة من الجرائم المنصوص عليها فيه».

لكن ارتكاب الجريمة داخل الإطار الاقليمى يحقق أيضاً فى الفروض التى يكون فيها الجانى خارج مصر ويرتكب الجريمة داخل القطر، وذلك حسب المادة ٢/١ من قانون العقوبات المصرى التى تنص على أنه:

«تسرى أحكام هذا التشريع على كل من ارتكب فى خارج القطر فعلاً يجعله فاعلاً أو شريكاً فى جريمة وقعت كلها أو بعضها فى القطر المصرى.

والعبرة فى تحديد إقليمية القاعدة الجنائية هى بوقوع الجريمة كاملة أو جزء

---

(*) القانون رقم ٥٨ لسنة ١٩٣٧ بإصدار قانون العقوبات.
الوقائع المصرية – العدد ٧١ الصادر فى ٥ أغسطس ١٩٣٧م.

منها على الأقليم المصرى (السلوك أو النتيجة)(١). وكذلك الحال فى الجرائم المستمرة والجرائم المتتابعة الأفعال، حيث يكفى أن يتحقق جزء من حالة الاستمرار أو فقرة من فقرات التتابع في مصر حتى يطبق القانون المصرى على الواقعة بأكملها(٢)، فمن حاز شيئاً مسروقاً وتنقل به فى أقاليم عدة دول، فإن جريمة الاخفاء تعتبر مرتكبة فى كل هذه الاقاليم، بغض النظر عن مكان وجود مرتكبها(*).

ويترتب على ذلك أن القانون المصرى يطبق على كثير من الجرائم المعلوماتية، طالما أن الاختصاص ينعقد لمجرد وقوع أحد العناصر المكونة للجريمة، أو حتى وقوع النتيجة على الاقليم. فيطبق على أفعال:

- الرسائل ذات الطابع الإجرامى، أو الصور الإباحية، أو العبارات التى تحض على الكراهية العنصرية والتى تنشر عبر شبكات الإنترنت.

بصرف النظر عن الدولة التى صدرت منها الرسالة، طالما أنه يمكن الدخول اليها فى مصر، وذلك لأن تلقى Réception المستخدم لهذه الرسالة أو تلك

---

(١) د/ جميل عبد الباقى الصغير – المرجع السابق – ص ٤٦.

(٢) د/ محمود نجيب حسنى – شرح قانون العقوبات (القسم العام) – دار النهضة العربية – ط ٤ – سنة ١٩٧٧ – رقم ١١٢ – ص ١٣٢، د/ مأمون سلامة – قانون العقوبات (القسم العام) – دار الفكر العربى – القاهرة – سنة ١٩٩٠ – رقم ٩ – ص ٧٤. وأيضاً يراجع:

- VIDAL (Georges), Cours de droit criminel et de science Pénitentiaire, 8 émé éd., mise à Jour Par MAGNOL (JEAN), Librairie Arthur Rousseau, Paris, 1935, Note 1, p. 1071.

وقد سبق أن أخذ القضاء الفرنسى بالنتيجة، فى جرائم الاعتداء على حق المؤلف لعقد الاختصاص للقانون الفرنسى.

- Ca. Paris, 30 Mars 1987, J.C.P. 1988, 2, 20965, note Bouzat (P.)

(*) كما أن ارتكاب الجريمة لا يقتصر على الحالات التى يكون فيها الشخص فاعلاً أصلياً، بل ينصرف أيضاً إلى الحالات التى يساهم فيها بوصفه شريكاً.

الصور على اقليمه، يعد أحد العناصر المكونة للجريمة، طبقاً لنص المادة ٢/١ عقوبات مصرى.

- التوصيل بالمعلومات غير المشروعة:

حيث يعد أحد العناصر المكونة للجريمة، فمجرد التوصيل يكفى لتحقيق ماديات الجريمة.

وبذلك يكون القانون العربى النموذجى قد أخذ بمبدأ - إقليمية النص الجنائى - فى تحديد القانون الواجب التطبيق بالنسبة لجرائم المعلوماتية، وهناك مبدأ عينية النص الجنائى، الذى طبقا له يمتد التشريع الجنائى للدولة ليطبق على الجرائم التى ترتكب فى الخارج بصرف النظر عن جنسية مرتكبيها[1]. حيث يستند هذا الامتداد إلى ما للدولة من حق فى الدفاع الذاتى، ضد كافة صور الاعتداء على مصالحها الأمنية والمالية ولو وقعت خارج إقليمها، خاصة وأن السلطات الأجنبية التى وقعت فوق اقليمها هذه الجرائم، قد تتقاعس عن ضبط فاعلها وملاحقته بالأدلة والبراهين، وإعمال نصوص القانون العقابى بحقه[*].

---

(١) د/ جميل عبد الباقى الصغير - المرجع السابق - ص ٥٣.

(*) أخذ قانون العقوبات المصرى بمبدأ العينية بالنسبة لجرائم معينة وردت على سبيل الحصر، فتنص المادة (٢/١ الفقرة الثانية) من هذا القانون على أن:

«تسرى أحكام هذا القانون أيضاً على الأشخاص الآتى ذكرهم» : -

ثانياً: كل من ارتكب فى خارج القطر جريمة من الجرائم الآتية:

أ - جناية مخلة بأمن الحكومة مما نص عليه فى البابين الأول والثانى من الكتاب الثانى من هذا القانون.

ب- جناية تزوير مما نص عليه فى المادة ٢٠٦ من هذا القانون.

جـ- جناية تقليد أو تزييف أو تزوير عملة ورقية أو معدنية مما نص عليه فقى المادة ٢٠٢ ع، أو جناية إدخال تلك العملة الورقية أو المعدنية المقلدة أو المزيفة أو المزورة إلى مصر أو.....

(الفقرة الأخيرة معدلة بالقانون رقم ٦٨ لسنة ١٩٥٦ - الوقائع المصرية العدد ٥٦ مكرر - الصادر فى فبراير ١٩٥٦).

ومن هذه الجرائم ما يمكن ارتكابة - بطبيعة الحال - عن طريق نظم المعلوماتية (الإنترنت) مثل جريمة السعى أو التخابر لدى دولة أجنبية (المواد ٧٧/ب، جـ، د،، عقوبات مصرى) وجريمة تسليم أو افشاء اسرار الدفاع عن البلاد (م ٨٠ عقوبات). وكذلك الجرائم المنصوص عليها فى المواد (٩٨/أ، ٩٨/ب، ١٧٤ عقوبات مصرى).

وبدراسة الفقرة الثانية من المادة (٢٢) من القانون العربي النموذجي المذكور، نتبين أن هذا القانون نص صراحة على سريان التشريع الجنائي – الوطني – على الجريمة المعلوماتية متى وقعت خارج الدولة، إذا كانت مخلة بأمنها – أي أمن الدولة – وذلك وفقاً للقواعد العامة المنصوص عليها في قانون العقوبات. وعلى ذلك يطبق القانون الجنائي المصري على جرائم المعلوماتية – الموجهة ضد مصر – متى وقعت خارج الدولة وكانت تخل بأمن الدولة (السياسي – العسكري – الاقتصادي)، وفقاً للقواعد العامة المنصوص عليها في قانون العقوبات المصري(١).

كما يلاحظ أن نص المادة (٢٢) من القانون العربي النموذجي لمكافحة جرائم الكمبيوتر والإنترنت، لم يأخذ بمبدأ شخصية النص الجنائي(*).

**ب- المحكمة المختصة:**

وفقاً لنص الفقرة الأولى من المادة (٢٢) من القانون النموذجي المذكور سابقاً، تختص المحاكم الوطنية بنظر الدعوى المترتبة على جرائم المعلوماتية، التي يطبق عليها قانون الدولة الوطني.

---

(١) د/ عبد الفتاح بيومي حجازي – مرجع سابق – ص ٥١.

(*) لمبدأ شخصية النص الجنائي وجهان:

- الوجه الايجابي Actif: يعني تطبيق النص الجنائي على كل من يحمل جنسية الدولة، ولو ارتكب جريمته خارج اقليمها.
- الوجه السلبي Passif: يعني تطبيق النص الجنائي على كل جريمة يكون المجني عليه فيها منتمياً إلى جنسية الدولة، ولو كان مرتكب هذه الجريمة أجنبياً وارتكبها خارج اقليم الدولة، والمقصود بهذا الوجه حماية رعايا الدولة اذا ما تعرضوا لاعتداء جرمي خارج نطاق دولتهم. (د/جميل عبد الباقي الصغير – المرجع السابق –ص ٥٥).

ولا يعرف المشرع المصري مبدأ شخصية النص الجنائي في وجهه السلبي، فجنسية المجني عليه ليست معياراً يحدد نطاق تطبيق النص الجنائي من حيث المكان. (د/محمود نجيب حسني – مرجع سابق – رقم ١٢٩ – ص ١٤٥).

ولكنه يعرف مبدأ شخصية النص الجنائي في وجهه الايجابي (م ٣ عقوبات).

وعلى ذلك متى كانت الجرائم المعلوماتية – أيا كان نوعها – وسواء وقعت على شبكة معلوماتية داخلية أو عن طريق شبكة الإنترنت، وسواء كان ذلك داخل الدولة أو خارجها شرط أن يكون القانون الوطنى صالحاً للتطبيق عليها، فإن المحاكم الوطنية هى المختصة دون غيرها بنظر هذه الجرائم.

- والاختصاص المكاني يتحدد وفقاً لضوابط ثلاث هي:

مكان وقوع الجريمة، أو مكن إقامة المتهم، أو مكان ضبطه (م ٢١٧ من قانون الإجراءات الجنائية ١٥٠ لسنة ١٩٥٠).

وهذه الأماكن الثلاثة للاختصاص المحلى متساوية لا تمييز بينها، والمحكمة التى ترفع إليها الدعوى تكون أولاً هى المختصة، ولأن السلوك والنتيجة يمثلان شطرى الجريمة. فإن كل من سلطات ومحاكم مكان النشاط الإجرامى ومكان النتيجة تكون مختصة(١).

وتطبيقاً لذلك فى نطاق الإجرام المعلوماتى.. فى جريمة بث الفيروس المعلوماتى، وتحقق الإتلاف لنظم المعلوماتية عن طريقه، إذا تم بث الفيروس المعلوماتى (السلوك الإجرامى) فى مكان، وتحققت النتيجة (تدمير المعلومات) فى مكان آخر، فإن الاختصاص ينعقد لمكان السلوك أو مكان حدوث النتيجة.

وبالنسبة لسلطة التحقيق فإنها تكون مختصة بالتحقيق فى حالة وقوع الجريمة كلها أو جزء منها فى دائرة الاختصاص المكانى سلطة التحقيق، أو إذا كان المتهم يقيم بتلك الدائرة أو كان قد تم القبض عليه فى ذات الدائرة. واذا كانت الجريمة المعلوماتية المرتكبة لها طابع الجريمة المستمرة، فإنها تعد وقد ارتكبت فى جميع الأماكن التى أمتدت الجريمة فيها(٢).

---

(١) د/ محمد محى الدين عوض – بحث عن مشكلات السياسة الجنائية المعاصرة فى جرائم نظم المعلومات – المؤتمر السادس الجمعية المصرية للقانون الجنائى – القاهرة – ٢٥: ٢٨ أكتوبر ١٩٩٣.

(١) د/ جميل عبد الباقى – المرجع السابق – ص ٦٣.

-/-

## الفرع الثاني

## تسليم المجرمين

إن إمكانية ارتكاب جرائم معلوماتية من خلال وحدة طرفيه فى دولة أجنبية أدت إلى ابتعاد المجرمين عن سلطات الدولة المتضررة من الجريمة، وافلاتهم من العقاب فى كثر من الاحيان. واحساساً بأهمية التعاون الدولى لمكافحة الجرائم عابرة الحدود – ومنها جرائم المعلوماتية – وضمان توقيع العقاب على مرتكبى هذه الجرائم، أبرمت معظم الدول اتفاقيات فيما بينها بشأن تسليم المجرمين، تهدف إلى قيام الدولة المطلوب إليها بتسليم أحد الأشخاص الموجودين على أقليمها إلى الدولة الطالبة لمحاكمته، أو تنفيذ عقوبة قضت بها عليه احدى محاكمها(١).

ويقوم مبدأ تسليم المجرمين على أساس، أن الدولة التى يتواجد على اقليمها المتهم بارتكاب احدى الجرائم عابرة الحدود مثل جرائم المعلوماتية، عليها أن تقوم بمحاكمته، اذا كان تشريعها يسمح بذلك، وإلا عليها أن تقوم بتسليمه لمحاكمته بمعرفة دولة أخرى مختصة(*).

والتسليم – بصفة عامة – هو اجراء تتخلى الدولة بموجبه، عن فرد موجود

---

== واذا كانت الجريمة المتعلقة بالإنترنت لها طابع الجريمة المستمرة، فهى تعد مرتكبة فى جميع الأماكن التى امتدت الجريمة فيها. مثال ذلك جريمة الدخول أو البقاء غير المشروع فى نظام المعالجة الآلية للمعلومات (م ٣٢٣-١ من قانون العقوبات الفرنسى الجديد). فتختص بالفصل فى هذه الجريمة جميع المحاكم التى تحققت فى دوائرها حالة الاستمرار.

أما اذا كانت الجريمة وقتية، كما فى حالة اتلاف المعلومات أو البرامج باستخدام القنبلة المنطقية Bombe logique، ينعقد الاختصاص للمحكمة التى وقعت الجريمة فى دائرتها.

(١) د/ جميل عبد الباقى الصغير – المرجع السابق – ص ٨٨.

(*) يختلف نظام تسليم المجرمين عن حق الدولة فى إبعاد الأجانب، أى طردهم من اقليمها بما لها من سيادة عليه، اذا ما قدرت أن وجودهم أو بقائهم على اقليمها من شأنه أن يؤثر على وجودها أو أمنها، وهو حق ثابت لكل دولة على ما أستقر عليه العرف الدولى، باعتباره إجراء داخلياً تمارس به الدولة سيادتها. (د/ على راشد – القانون الجنائى [المدخل – وأصول النظرية العامة] بدون ناشر – سنة ١٩٧٤ – ص ٢٠٢).

لديها لسلطات دولة أخرى – تطالب بتسليمه إليها – بغرض محاكمته عن جريمة ارتكابها، أو لتنفيذ حكم صادر ضده بعقوبة جنائية[1].

والغرض من التسليم هو الحيلولة دون إفلات المجرم من العقاب، فى حالة ما اذا كان القانون الداخلى للدولة المتواجد على اقليمها المتهم لا يسمح لتلك الدولة بمحاكمته عن جريمته. وبالتالى فإن تسليم المجرمين هو أحد مظاهر التعاون الدولى فى مجال مكافحة الاجرام المعلوماتى.

**اولاً: شروط تسليم المجرمين[2]:** وضعت الاتفاقيات الدولية عدة شروط لتسليم المجرمين، بعضها يتعلق بالشخص المطلوب تسليمه، والبعض الآخر يتعلق بالجريمة محل التسليم. فلا يجوز التسليم فى الجرائم السياسية(*)، حيث يكون الغرض منه اتخاذ إجراءات انتقامية ضد الشخص المطلوب تسليمه، وهو عمل لا يليق بالدولة المطلوب منها التسليم أن تساهم فى تنفيذه.

واستناداً إلى هذا الشرط ترفض الدول المنضمة إلى الاتفاقية الأوربية للتعاون، تسليم المجرمين بذريعة أن من شأن التسليم في جرائم معينة مساس بمصالحها الاساسية. ومن أمثلة الجرائم المعلوماتية التى تشكل مساساً بالمصالح الاساسية للدولة، جريمة الدخول بطريق غير مشروع L'accés illicite عن طريق الشبكات الدولية أو الجامعية Par le biais des rèseaux internationaux et universitaires إلى قواعد البيانات الاستراتيجية Bases de donnégiques Stratégiques أو العلمية Scientifiques أو الاقتصادية Economiques أو المالية Financières[3].

---

(١) يراجع بشأن تسليم المجرمين:
د/ محمد الفاضل – محاضرات فى تسليم المجرمين – معهد الدراسات العربية بالقاهرة – سنة ١٩٦٦، ص ١٩، د/ محمود حسن العروس – تسليم المجرمين – رسالة دكتوراة كلية الحقوق – جامعة القاهرة –سنة ١٩٥١.

(٢) د/ جميل عبد الباقى الصغير – المرجع السابق – ص ص ٨٩ ، ٩٠.

(*) تحظر المادة ٥٣ من الدستور المصرى تسليم اللاجئين السياسيين.

(3) VERGUCHT (P.), op. cit., N$^{0}$, 336, p. 416

ومما لا شك فيه أن رفض التسليم فى مثل هذه الحالات قد يكون عقبة، تحول دون التعاون الدولى فى هذا المجال.

ويشترط لقيام مصر بتسليم شخص ما إلى دولة أجنبية، أن يكون الفعل المنسوب إلى هذا الشخص ارتكابه يشكل جريمة فى قانون الدولة طالبة التسليم وفى القانون المصرى معاً(*). كما يجب أن يكون الفعل على درجة معينة من الجسامة (جناية – أو جنحة)، وأن يكون معاقباً عليه بعقوبة سالبة للحرية(١).

---

(*) بمعنى أن الدولة المطلوب اليها التسليم، قد ترفض تقديم المساعدة لأنها ترى عدم لزوم معاقبة شخص عن فعل لا يشكل جريمة فى تشريعها.

(١) د/ عبد الرءوف مهدى، شرح القواعد العامة لإجراءات الجنائية، مرجع سابق – رقم ٤٠، ص ٨٨، د/ سالم محمد سليمان الأوجلى، مرجع سابق، ص ٤٣٨.

وتشترط بعض الأتفاقيات الدولية أن تكون الجريمة موضوع المحاكمة معاقب عليها بعقوبة سالبة للحرية مدتها سنة على الأقل، وأن يكون الحكم الصادر بالادانة والمطلوب تنفيذه يقضى بالحبس لمدة أربعة شهور على الأقل. وهو الأمر الذى ينطبق على معظم الجرائم المعلوماتية.

- VERGUCHT (P.), op. cit., N$^{0}$, 336, p. 415.

ولا يعترف القانون المصرى الحالى للحكم الأجنبى بقوة تنفيذية بالنسبة للعقوبات الأصلية التى يقضى بها، ولكن قد يكون هذا الاعتراف بناء على معاهدات دولية (مثل ذلك اتفاقية تسليم المجرمين بين دول الجامعة العربية الموقع عليها فى ٩ يونيو سنة ١٩٥٣، والمصدق عليها من مجلس الوزراء فى ٣ نوفمبر سنة ١٩٥٤، اعتباراً من ٢٨ أغسطس سنة ١٩٥٤)، كما لا يعترف القانون الحالى للحكم الأجنبى بقوة تنفيذية بالنسبة لاثارة الثانوية، وذلك إلا اذا كانت هناك نصوص خاصة وفى حالات محددة (انظر المادتان ٤، ٧ من القانون رقم ٥٨٣ لسنة ١٩٥٥ فى شأن تنظيم المدارس الحرة). ويعترف القانون السارى للحكم الاجنبى بقوة الشئ المحكوم فيه بشروط معينة تنص عليها المادة ٤ من قانون العقوبات، حيث لا يجوز اقامة الدعوى الجنائية ضد مرتكب الجريمة فى الخارج اذا حوكم أمام المحاكم الأجنبية وقضى نهائياً ببراءته أو بادانته واستوفى عقوبته. وعله ذلك هى احترام قوة الشئ المحكوم فيه، اذ لا يجوز أن يحاكم شخص مرتين من أجل فعل واحد Non bis in idem. وعلى ذلك ينحصر مفعول الحكم الأجنبى أمام القضاء المصرى فى كونه مانعاً يحول دون رفع الدعوى الجنائية مرة ثانية ضد مرتكب الجريمة فى الخارج، اذا حوكم أمام المحاكم الأجنبية وقضت نهائياً ببراءته أو بادانته واستوفى العقوبة.

وهذا هو الحال أيضاً بالنسبة لفرنسا التى لا تعترف بالأحكام الجنائية الأجنبية، وترفض تنفيذها Versailles, 10 Octobre 1983, D. 1984, I.R., p. 87. فالحل الوحيد لتنفيذ الأحكام الأجنبية هو أن تكون هناك اتفاقيات دولية فى هذا الشأن.

ويشترط كذلك أن يكون قانون الدولة طالبة التسليم مختصاً بمحاكمة الشخص المطلوب تسليمه إليها، وإلا انتفى الغرض من التسليم[١].

ومع ذلك فإن شرط ازدواج التجريم قد يكون عقبه فى مجال تسليم المجرمين، لأننا اذا رجعنا إلى التشريعات الجنائية الوطنية لوجدنا أن جرائم المعلوماتية غير معاقب عليها فى معظم الدول من ناحية، وأنه من الصعب أن نحدد فى تشريعات الدولة المطلوب إليها التسليم، ما اذا كانت النصوص التقليدية لديها يمكن أن تطبق على جرائم شبكات الحاسبات الآلية والإنترنت من عدمه، من ناحية أخرى. بمعنى أنه من الصعب البحث فى تشريعات الدول المطلوب اليها التسليم عما إذا كانت تشريعاتها الجنائية التقليدية يمكن أن تطبق على جرائم المعلوماتية، وبالتالى يتوافر شرط ازدواج التجريم أم لا. يضاف إلى ذلك ان الدول قد تفسر بتوسع شرط ازدواج التجريم، الأمر الذى يعوق تطبيق الاتفاقيات الدولية فى مجال تسليم المجرمين، ويحول بالتالى دون جمع الأدلة ومحاكمة مرتكبى الجرائم المتعلقة بالمعلوماتية[٢].

ولذلك يجب أن يكون هناك تنسيق أو توحيد بين التشريعات المختلفة فيما يتعلق بتعريف الجرائم المعلوماتية، والجرائم المتعلقة بالانترنت، أو على الأقل عدم اشتراط ازدواج التجريم. وتوجد بالفعل بعض الاتفاقيات الدولية الثنائية التى تحدد الجرائم التى لا تتطلب فيها شرط ازدواج التجريم ومنها جرائم المعلوماتية. مثال ذلك الاتفاقية الثنائية المتعلقة بالمساعدة القانونية المتبادلة والتى تم توقيعها بين امريكا وكندا، والتى لم تتطلب ازدواج التجريم كشرط للتعاون القضائى الدولى فيما بينهما. وتدخل جرائم المعلوماتية فى اطار هذه الاتفاقية[٣].

---

(١) د/ عبد الرءوف مهدى – شرح القواعد العامة للإجراءات الجنائية – المرجع السابق – رقم ٤١ – ص ٩٥.

(2) VERGUCHT (P.), op. cit., N$^0$, 334, pp. 414 - 415.

(3) In The Place Cited.

**ثانياً: إجراءات طلب التسليم:** يجب أن يقدم طلب التسليم من حكومة الدولة الطالبة إلى الحكومة المصرية عن طريق وزارة الخارجية المصرية (أى بالطرق الدبلوماسية)، والتى تحيله بعد فحصه من الناحية السياسية إلى وزارة العدل للنظر فيه وتقرير مدى أحقيته. ويجب أن يرفق بطلب التسليم بيان بالأفعال المطلوب التسليم من أجلها، وزمان ومكان ارتكابها، وتكييفها القانونى والنصوص الواجبة التطبيق. واذا كان الغرض من التسليم هو تنفيذ عقوبة على الشخص المطلوب تسليمه، فيجب أن يرفق بطلب التسليم صورة رسمية من الحكم القضائي البات الصادر بالإدانة، وذلك حتى يتم التحقق من توافر شروط التسليم طبقاً للاتفاقيات في هذا الصدد[1].

ويمكن أن يقدم طلب التسليم من الدولة الطالبة كتابة إلى النائب العام، الذى يكون له سلطة الفصل فى هذا الطلب بالموافقة أو الرفض. وفى حالة طلب مصر تسليم شخص من دولة أجنبية، فإن النائب العام هو الذى يطلب إلى وزير العدل توجيه الطلب الى السلطات المختصه فى الدولة الأجنبية، ويبلغ الطلب بالطرق الدبلوماسية[2].

**ثالثاً: اتفاقيات تسليم المجرمين (علي المستوي الدولي)[3]:**

مجموعة من الاتفاقيات في مجال تسليم المجرمين يبدو لأول وهله أنه يمكن تطبيقها فى مجال الجرائم المعلوماتية عابرة الحدود(*)، على اعتبار أن

---

(١) د/ جميل عبد الباقي الصغير – المرجع السابق – ص ٩٢.

(٢) د/ عبد الرءوف مهدى، شرح القوعد العامة للإجراءات الجنائية، المرجع السابق، رقم ٤٢، ص ص ٩٧ – ٩٩.

(٣) د/ جميل عبد الباقى الصغير – المرجع السابق – ص ٩٣.

(*) وقعت مصر على اتفاقية تسليم المجرمين المبرمة بين دول الجامعة العربية فى ٩ يونيو سنة ١٩٥٣ (وافقت عليها بالقانون رقم ٨٣ لسنة ١٩٥٤)، واتفاقية نقل المحكوم عليهم بعقوبات سالبة للحرية مع تركيا فى ٢٣ مارس سنة ١٩٨٧، والاتفاقية الخاصة بنقل المحكوم عليهم بعقوبات سالبة للحرية مع اليونان فى ١١ يونيو سنة ١٩٨٧، والاتفاقية المعقودة مع المجر فى

-/-

هذه الاتفاقيات لم تأخذ فى الاعتبار الأساليب التقنية لارتكاب الجرائم، ولا يبين منها أنها تخص فئة معينة من المجرمين. ومع ذلك فإن هذه الآليات للتعاون Coopération بين الدول غير فعالة، باعتبار أن كل الدول ليست منضمة إلى هذه الاتفاقيات. كما أن تطبيقها قد يصطدم بعقبات، تتمثل فى أن الجريمة المطلوب تسليم مرتكبيها لمحاكمتهم قد تكون ذات طابع سياسى.

وعلى ذلك فإن التعاون القضائى الدولى بات أمراً ضرورياً لمكافحة المواقع غير المشروعة، والرسائل المجرمة التى تبث على شبكة المعلومات، نعم هناك تقدم فى هذا المجال، إلا أنه تقدم يسير بخطى بطيئة والدول متحفظة فى ابرام الاتفاقيات خشية التأثير على سيادتها. ومع ذلك فإن مكافحة جرائم تكنولوجيا المعلومات قد تضطر الدول إلى النزول عن جزء من سيادتها فى سبيل بلوغ هذا الهدف. ويتحقق ذلك عن طريق ابرام اتفاقيات دولية جماعية بغرض.

١- اتخاذ التدابير الملائمة لحل مشكلات الاختصاص القانونى والقضائى، التى تثيرها جرائم المعلوماتية عابرة الحدود.

٢- تنظيم اجراءات التفتيش وضبط المعلومات التى تعبر شبكات الإنترنت، مع كفالة الحماية – فى الوقت نفسه – لحقوق الأفراد وحرياتهم وسيادة الدول.

٣- تطوير أدلة الإثبات بما يتلائم مع هذا الشكل الجديد والمعقد، من النشاط الإجرامى (جرائم المعلوماتية – والجرائم الافتراضية).

٤- تسليم المجرمين وتبادل المساعدة، فى المسائل المرتبطة بجرائم تكنولوجيا المعلومات عابرة الحدود.

--- ٢٦ مارس سنة ١٩٨٨، والخاصة بالمساعدة القضائية وتسليم المجرمين ونقل المحكوم عليهم، واتفاقية نقل المحكوم عليهم بعقوبات سالبة للحرية مع الكويت فى ٩ يناير ١٩٩٠، واتفاقية التعاون القضائى فى المواد الجنائية ونقل المحكوم عليهم وتسليم المجرمين مع بولندا فى ١٧ مايو سنة ١٩٩٢. (د/ عبد الرءوف مهدى – المرجع السابق – هامش ٣٠، ٣١ – ص ٨٥).
وفى اطار المجلس الأوروبى أبرمت فرنسا اتفاقية تسليم المجرمين فى ١٣ سبتمبر ١٩٥٧، ثم أضيفت اليها مجموعة من النصوص التكميلية.

- VERGUCHT (P.), op. cit., N$^{0}$, 331, p. 411.

# الخاتمة

# (الخاتمـة)

يطلب لى أن أبدأ تسطير الخاتمة بكلمات هى بحق معبرة، فحواها أنه ليس الغرض من الخاتمة تلخيص الدراسة واستعراض أبوابها، وما تضمنته من فصول ومباحث بشكل بانورامى يلم بكل شاردة وواردة، فهذا أمر يجاوز حدودها، وإنما الغرض منها إبراز مغزى الدراسة(*).

ونضيف إلى هذه التضاعيف(**) أن الخاتمة تحوى فكر الباحث ورؤيته لموضوع البحث، وتعج بخلاصة العمل القانونى، فهى – إن صح الوصف والتشبيه – نهاية المطاف وكشف النقاب الذى يأتى فى نهاية العمل الفنى (حيث الخاتمة أهم أجزاء الفيلم)، أو تسليط الضوء على بطل العمل المسرحى فى نهاية العرض، وهو يجسد مغزى هذا العمل مع اسدال ستائر التياترو.

وقد تناولت الدراسة موضوع الأمن المعلوماتى، مشيدت أركان هذا الموضوع برؤية النظام القانونى لحماية المعلوماتية Systéme Judiciaire pour la Protection de L'informatique. فالقانون هو الأمن للمجتمع، وتطبيق القانون يعنى الآمان لمواطنى المجتمع، وسن التشريعات هو الوجه الأخر لعملة حماية المجتمع، وإرساء لمبادئ الدولة القانونية الحريصة على صلاح مجتمعها وحماية مواطنيها.

وقد أنقسمت الدراسة إلى بابين رئيسيين، سبقهما فصل تمهيدى بيانهم:

**الفصل التمهيدي: الأمن والمعلوماتية:**

تم من خلاله استعراض ماهية الأمن ثم ماهية المعلوماتية، وماهية الشئ التعريف به وبعناصره التى يتكون منها.

---

(*) من العبارات المأثورة للأستاذ الدكتور/ محمد ذكى أبو عامر، سطرها فى خاتمة البعض من مؤلفاته القانونية.

(**) التضاعيف: السطور.

**الباب الأول: الحماية الموضوعية للمعلوماتية:**

وتم من خلال هذا الباب عرض لماهية الجريمة المعلوماتية، وخصائصها، وسمات المتهم المعلوماتي، في تمهيد سبق ما أشتمل عليه هذا الجانب من الدراسة، من فصلين رئيسيين:

**الفصل الأول: الجريمة المعلوماتية في القانون:**

حيث تم عرض لتقسيم الجريمة المعلوماتية، وتبع ذلك عرض للتنظيم القانوني لصور الاعتداء على نظم المعلوماتية (الجرائم المعلوماتية).

**الفصل الثاني: الجريمة المعلوماتية في الاتفاقيات الدولية:**

تم من خلال هذا الفصل عرض لنماذج الجرائم المعلوماتية التي تضمنتها أتفاقية بودابست ٢٠٠١ للإجرام المعلوماتي، واتفاقية المجلس الأوروبي ٢٠٠٤ بشأن الجريمة المعلوماتية.

**الباب الثاني: الحماية الإجرائية للمعلوماتية:**

نظراً لأهمية الجانب الإجرائي في العمل القانوني، وضرورة أصباغه بالشرعية القانونية، فقد تم في بداية القسم الثاني من الدراسة ايضاح مفهوم الحماية الإجرائية، وتبعنا ذلك بعرض للشرعية الإجرائية المقصودة في مواجهة الجرائم المعلوماتية. وتلى ذلك:

**الفصل الأول: الحماية الإجرائية القانونية للمعلوماتية:**

تم من خلال هذا الفصل تفصيل إجراءات مواجهة الجريمة المعلوماتية (من تفتيش وضبط، وعرض للمشكلات العملية أثناء تنفيذ هذه الإجراءات)، ثم عرض للحماية الإجرائية للمعلوماتية في ضوء الاتفاقيات الدولية.

**الفصل الثاني: الحماية الفنية للمعلوماتية:**

تم فى تمهيد الفصل عرض للبعد الاستراتيجى لأمن المعلومات، ثم ايضاح وسائل اختراق نظم الأمن المعلوماتى، وتبع ذلك عرض لوسائل حماية المعلوماتية، القانونية والفنية والدولية.

وخلصنا فى دراستنا إلى أننا نعيش اليوم فى عصر المعلوماتية المتشعبة، الممزوجة بالإعلام الفورى، إعلام يطلق وابلاً متصلاً من الصور والرموز (الحقائق) المتصارعة. وكلما ازدادت البيانات والمعلومات والمعرفة التقنية المستخدمة فى شتى مناحى الحياة – حيث التوغل أكثر داخل مجتمع المعلومات، – قد تصبح معرفة حقيقة الأمور والوقوف على اعتاب وصدق الوقائع والأحداث، من الصعاب بالنسبة للجميع.

وقد تعرض الفقه والبحث كثيراً للجرائم التقليدية، ثم تبع ذلك أرهاصات للجريمة المستحدثة (الجريمة الافتراضية والمعلوماتية)، وسطر الجميع جانب من أساليب المعلوماتية التى تطمس – وتشوه – صورة الحقيقة فى أذهان الجميع من خلال أساليب متعمدة – تمثل اعتداء على نظم المعلوماتية – أو غير متعمدة من خلال معلومات مغلوطة أو متحيزة أو مشبوه. ويتشكك الباحث – الفقيه – الفاحص للأمور فى مدى موضوعية وسائل المعلوماتية للوصول إلى الحقائق المبتغاه، حيث أن هناك مستوى أعمق من التشويه لنظم المعلومات، لم ينل حظاً يذكر من الدراسة والتحليل والفهم والاستنباط، ذلك الذى يستهدف مستقبل الأمة.

وفى هذا السياق أثارت الجرائم المستحدثة – الافتراضية – ومنها جرائم المعلوماتية تحديات جسيمة فى التشريعات القانونية، وخاصة بالنسبة لقانون العقوبات. ويرجع السبب فى المسألة إلى أن القوانين الجزائية – العقوبات – كانت حتى وقت قريب، تبسط حمايتها على الوقائع المادية والمرئية (وما تشمله من أشياء وتصرفات)، أما بالنسبة للمعلومات والقيم – الأمور – المعنوية

الأخرى المرتبطة بها، التى ظهرت فى النصف الأخير من القرن الماضى، فلم تشملها هذه الحماية إلا فى حدود ضيقة، وبفكر تقليدى يعتمد على القواعد القانونية العامة.

وهناك العديد من التشريعات الغربية (خاصة فى الدول المتقدمة) التى تضمنت نصوصاً خاصة بهذا النوع من الجرائم، ظهرت فى السنوات القليلة الماضية، حيث جرمت الأفعال غير المشروعة التى تمثل انتهاكاً لحقوق الآخرين المعلوماتية.

فيما خلت تشريعات العديد من الدول – خاصة الدول النامية ومنها أغلب الدول العربية – من أية نصوص تجرم تلك الأفعال، تاركة الأمر لاجتهاد القضاء، استناداً إلى القواعد العقابية العامة.

وفى نطاق البُعد الاستراتيجى لأمن المعلومات تبرز موضوعات هامة، منها التعاون الدولى فى أطر المعلوماتية، ومصطلح تكتيك المعلومات وأهميته فى المجتمع المعلوماتى، والعلاقة بين المعلوماتية وعصر تحول السلطة.

- **التعاون الدولي في أطر المعلوماتية:**

من الأهمية أن تتألف الدول المعنية فيما بينها، حتى يمكن اتخاذ الإجراءات القانونية – من ضبط الجناة، وإقامة الدليل المعلوماتى، وإجراء المحاكمات – بالنسبة للجرائم المعلوماتية، وخاصة أن الأمر يتعلق بنوع من الجرائم عابرة للحدود. وفى ذات الاتجاه شدد المجلس الأوروبى منذ سنة ١٩٨٩ على ضرورة تدويل Internationalisation جرائم التكنولوجيا، وخاصة تلك المتعلقة بالمعلوماتية(*).

---

(*) فى سنة ١٩٨٩ أقر مجلس الوزراء الأوروبى توصية تحث الدول الأعضاء على الأخذ فى الاعتبار المبادئ الرئيسية التى نادى بها المجلس الأوروبى. وفى ١١ سبتمبر سنة ١٩٩٥ أقر وزراء المجلس الأوروبى التوصية R 95-13 المتعلقة بمشاكل الإجراءات الجنائية المرتبطة

-/-

● تكتيك المعلومات:

يعنى هذا المصطلح مناورات الجهات المختصة - السلطة القائمة - على تطويع المعلومات، غالباً قبل أن تصل إلى وسائل الإعلام، وسوف تكتسب هذه التكتيكات أهمية كبرى فى حياة الشعوب - خاصة الحياة السياسية، بازدياد أهمية المعرفة بكل أشكالها، وبتراكم البيانات والمعلومات والمعرفة وتدفقها من الحاسبات الآلية، وفى الأزمات المقبلة - وخاصة السياسية - التى تواجه الدول - الديمقراطية ذات التقنية المتقدمة سيتم استخدام «تكتيكات المعلومات» من قبل كل الأطراف، من جهات حكومية ومسئولين - سياسيين - ولوبى الشركات والمد المتزايد من جماعات المواطنين(١).

وفى نطاق الأمن المعلوماتى والحفاظ على سرية جانب هام من المعلومات والبيانات، يبرز «تكتيك السرية» كأول - وربما أقدم - تكتيكات المعلومات وأكثرها انتشاراً. ويعنى هذا المعنى تصنيف الجهات الحكومية - أو الكيانات الاقتصادية - لمستندات على أنها سرية، وأغلب هذه المستندات مرتبط إما بالشئون العسكرية أو الدبلوماسية أو الاقتصادية - أو بأمور وموضوعات قد يتحرج منها المسئولون - فماذا يكون الوضع عند أختراق هذه المعلومات

--- بتكنولوجيا المعلومات Liées à la technologie de l'information. وقد حثت هذه التوصية الدول الأعضاء على مراجعة قوانين الاجراءات الجنائية على ضوء المبادئ التى وضعتها وهى: ١- تفتيش الأنظمة المعلوماتية وضبط البيانات. ٢- الرقابة الفنية التقنية من أجل التحقيق الجنائى، ٣- الإلتزام بالتعاون مع سلطات التحقيق، ٤- الإجراءات والوسائل الفنية التقنية لمعالجة الدليل الالكترونى.

BENSOUSSAN Alain (Sous la direction de), Internet. Aspects juridiques, op. cit., p. 203, TORTELLO (N.) et LOINTIER (P.), Internet poru les juristes, Dalloz, Paris, 1996, Annexe 4.

(١) ألفن توفلر - تحول السلطة (بين العنف والثروة والمعرفة) - تعريب وترجمة د/ فتحى حمدين شتوان، نبيل عثمان - مكتبة طرابلس العلمية العالمية - ليبيا - ط٢ - سنة ١٩٩٦م - ص ٣٤٥.

وأفشائها، أو تسريبها إلى جهات معينة(*)، فالموضوع جد خطير ولا تقتصر آثاره على جريمة ارتكابها فرد، فمن الجائز أن يكون خلف هذه الجريمة كيان متكامل - سواء سياسى أو مخابراتى أو اقتصادى - وحتى الآن لم تشمل الحماية التشريعية للعديد من الدول هذه الأفعال، تاركين الأمر بأكمله للقواعد العامة(**).

- **المعلوماتية والمعرفة وعصر تحول السلطة:**

تبقى السلطة واحداً من أقل جوانب حياتنا خطأ من الفهم، وإن كان أكثرها أهمية لا سيما بالنسبة لجيلنا(***). ونقف الآن على اعتاب عصر تحول السلطة، إننا نمر بفترة بدأ يتفكك فيها كل هيكل السلطة الذى كان يجمع العالم بعضه

---

(*) بعض الأسرار المعلوماتية تكتم وبعضها تسرب - عندما يكون تسرب السر عملاً غير مقصود، فهو سر لم يحسن كتمانه. أما الأسرار المسربة بعناية - أى عمداً - فهى صواريخ معلوماتية موجهه يتم إطلاقها عن وعى وإدراك، لتصيب هدفاً محدداً أو أهدافاً محددة بدقة. (المرجع السابق - ص ٣٤٧).

(**) من نماذج اختراق الأمن المعلوماتى وتهديد كيانات وحكومات كبرى:

- ما اتاحته المعلومات المسربة فى فضيحة شركتى (ريكروت وكوزموس) المالية، من نتائج مدهشة فى اليابان، حيث آدت إلى استقالة رئيس الوزراء نوبورو تاكيشيتا فى عام ١٩٨٩. والمعلومات المسربة من مكتب المدعى العام الى الصحف اليومية - كانت بمثابة حركات فى باليه للسلطة بارع الأخراج - حالت دون شل التحقيقات وحماية عناصر الفساد فى حكومة تاكيشيتا.
- وفى فرنسا ظلت المعلومات المسربة تلعب طوال تاريخها دوراً سياسياً هاماً، ومنها عرض الصعوبات التى واجهتها فى إخراج نفسها من حرب الهند الصينية، وكان ذلك تكتيكاً سياسياً محلياً مقبولاً.
- وفى واشنطن أدت المعلومات المسربة بعناية من مصدر غير معروف حتى الآن يسمى (الحنجرة العميقة)، إلى إجبار ريتشارد نيكسون على الاستقالة من رئاسة الولايات المتحدة، فى فضيحة ووترجيت. (المرجع السابق - ٣٤٨).

(***) رغم السمعة السيئة التى تقترن بفكرة السلطة نفسها نتيجة لما ظلت تتعرض له من سوء استخدام، إلا أن السلطة فى حد ذاتها ليست بالشئ الحسن ولا السيئ. إنها جانب لابد منه فى أى علاقة إنسانية. وهى تؤثر على كل شئ، بدءاً من علاقاتنا الزوجية وانتهاء بالوظائف التى نستغلها والسيارات التى نقودها، والإذاعة المرئية التى نشاهدها والآمال التى نسعى لتحقيقها. وما نحن سوى نتاج للسلطة إلى حد يفوق ما يتصوره أغلبنا.

ببعض، وثمة هيكل للسلطة يختلف اختلافاً جذرياً آخذ الآن فى التشكل... ويحدث هذا على كل مستوى من مستويات المجتمع الإنسانى(*). وهذا التمزق الذى يشهده النمط القديم للسلطة والنفوذ على مستوى العمل والحياة اليومية، بات يتسع ويتزايد فى نفس الوقت الذى تتفكك فيه هياكل السلطة على مستوى العالم(**).

وثمة دافع قوى للاعتقاد بأن القوى التى تهز السلطة الآن على كل مستوى من مستويات النظام الإنسانى سوف تصبح أشد ضراوة، وأكثر تأثيراً فى السنوات القليلة المقبلة، هذه العملية الكبرى لإعادة هيكلة علاقات السلطة ستؤدى - كما يحدث عند تحرك الطبقات الأرضية وتطاحنها قبيل الزلزال - إلى واحدة من أندر الوقائع فى تاريخ الإنسان.. وهى حدوث ثورة فى طبيعية السلطة نفسها. إن «تحول السلطة» لا يعنى مجرد نقل السلطة، بل أيضاً تغيير طبيعتها. بمعنى.. إن التحول فى السلطة لا يعنى مجرد انتقالها من طرف إلى طرف أخر أقوى ليمارس هيمنته وتسلطه على المجتمع، بل يعنى تغيير طبيعتها كنتيجة طبيعية ولازمة لظهور عامل حيوى فى تكوين السلطة، وهذا العامل هو «المعرفة»(1).

---

(*) الأنماط القديمة للسلطة فى مكاتبنا ومتاجرنا ومصارفنا ومظاهر حياتنا بدآت الآن تتشقق فى خطوط جديدة غريبة. والصراعات العرقية والعنصرية آخذة فى التضاعف. وفى عالم الأعمال ترى الشركات العملاقة تتعرض للتفكيك ثم التجميع مرة أخرى، بعد أن تتهاوى آسهمها ومعها وظائف الآلاف من مستخدميها.

(**) لا يقتصر التحول فى السلطة على من يحتلون قمة الشركات فحسب، بل إن مديرى المكاتب وكذلك المشرفين على عنابر الإنتاج بدأوا يكتشفون أن العمال ما عادوا يتقبلون الأوامر على علاتها. كما كان يفعل الكثيرون منهم ذات يوم - بل باتوا يوجهون الأسئلة ويطالبون باجابات عليها، ويجابه ضباط الجيش نفس الشئ مع جنودهم، ورؤساء الشرطة مع رجالهم، والمدرسون - بصورة متزايدة - مع تلاميذهم.

(1) ألفن توفلر - تحول السلطة (بين العنف والثروة والمعرفة) - مرجع سابق مترجم - ص 16.

* والمفكر آلفن توفلر هو الذى أطلق مصطلح الموجة الثالثة... ظهر عام 1980، كان ذو تركيز مختلف، إذ عنى بشرح أحداث التغيرات الثورية فى التقنية والمجتمع ويوضعها فى المنظور التاريخى وباستشراق المستقبل الذى يمكن أن تتمخض عنه. وقد وصف المؤلف التغيرات

-/-

بيد أن ثمة معنى أوسع لما تسببه (أو تسهم فيه) التغيرات فى المعرفة من تحولات للسلطة والنفوذ. لقد كان أهم تطور اقتصادى فى زماننا هذا هو ظهور نظام جديد لخلق الثروة لا يقوم على العضلات - كما كان الحال فى السابق - بل على العقل. فلم يعد العمل فى الاقتصاد المتطور قاصراً على التعامل مع (الأشياء)، إنما كما يقول المؤرخ (مارك بوستر Mark Poster) بجامعة كاليفورنيا على «تأثير الرجال والنساء على رجال ونساء غيرهم.. أو - بمعنى أخر - تأثير الناس فى المعلومات وتأثرهم بها».

إن إحلال المعلومات أو المعرفة محل الجهد العضلى هو الذى يقف - فى الواقع - وراء متاعب شركة عملاقة مثل جنرال موتوز(*) .. وصعود دولة مثل اليابان(**). ذلك لأنه فيما كانت جنرال موتورز لا تزال تعتقد بأن الأرض مسطحة، كانت اليابان تستكشف حوافها وتكتشف أنها ليست كذلك، وعلى الرغم من أن الولايات المتحدة كان لها سبق البدء فى استخدام الحاسب الآلى، إلا أن اليابان كانت أسرع منها فى احلال تقنيات الموجة الثالثة القائمة على المعلومات، محل التقنيات القائمة على المجهود العضلى المنتمية للموجة الثانية.. المنحسرة.

---

= الاجتماعية والتكنولوجية الهامة التى بدأت فى منتصف الخمسينات بأنها موجة ثالثة كبرى من موجات التغيير البشرى - بداية مدنية جديدة تالية لعصر المصانع ذات المداخن، وقد أشار ضمن أشياء أخرى، إلى صناعات جديدة آتية تقوم على الحاسبات الآلية والإلكترونية والمعلومات والتقنية الحيوية ... وما شابه ذلك، وأطلق على هذه أسم (المرتفعات القيادية الجديدة) للاقتصاد. كما تنبأ بأشياء مثل التصنيع المرن والأسواق الصغيرة الملائمة (Niche Markets)، وأنتشار العمل الجزئى (أى غير المتفرغ له) وتفكك جماعية وسائل الاعلام.

(*) قبل عشرون عاماً كانت جنرال موتورز تعد الشركة الصناعية الأولى فى العالم، ونموذجاً متألقاً يتطلع إليه المدراء فى أقطار المعمورة.. كما كانت بؤرة للنفوذ السياسى فى واشنطن؛ أما اليوم فإنها (تلهث من أجل البقاء) على حد قول أحد كبار المسئولين فيها، وليس من المستبعد أن نرى تفكك جنرال موتوز فى السنوات المقبلة.

(**) مع انتشار سلطة الحاسب الآلى سريعاً فى أرجاء العالم، أنتفضت الشركات اليابانية ودخلت منافسات ضارية مع نظائرها من شركات عالمية فى العالم، وباتت قوة اليابان الاقتصادية تنطلق إلى عنان السماء.

ومنذ عام ١٩٧٠ ، حينما كان قادة الأعمال فى أمريكا لازالوا، يعتقدون بأن صناعاتهم ذات المداخن فى أمن وأمان، كان نظراؤهم فى اليابان، بل وعامة جمهورهم يتعرضون لسيل لا ينقطع من الكتب والمقالات الصحفية والبرامج المرئية، التى تبشر بمقدوم (عصر المعلومات) وتركز على القرن الحادى والعشرين.

إن انتشار الاقتصاد الجديد المبنى على المعرفة، إنما يمثل – فى الواقع – القوة التفجيرية الجديدة التى قذفت بالدول المتقدمة إلى أتون التنافس العالمى المرير، وكشف للأقطار الشيوعية عن التخلف المزمن لصناعاتها، وأجبرت كثيراً من (البلدان النامية) إلى التخلى عن استراتيجيتها الاقتصادية التقليدية.. وهى الآن تزعزع علاقات السلطة والنفوذ على المستويين الشخصى والعام.

لقد قال ونستون تشرشل – كما لو كان يقرأ الغيب – بأن:

(إمبراطوريات المستقبل ستقوم على العقل). واليوم أضحت تلك الملاحظة حقيقة واقعية(١).

ولكن هذه نظرة قاصرة عمرها بضع سنوات، لأن إحكام العقل والفكر وإعمال المعرفة أساسيات وركائز حثت عليها الشرائع السماوية، وقد زخر القرآن الكريم بالآيات القرآنية الكريمة التى توضح أهمية العلم والمعرفة والتفكر والتدبير والتعقل فى حياة الإنسان، الذى ملك الدنيا بأسرها، وصال وجال بين ربوعها. إن العلم والمعرفة من الأمور الحاسمة فى الحكم، سواء الحكم على الأمور والمسائل، أو الحكم بمعنى التسيد والقيادة.

وفى سبيل تأكيد ذلك نتوقف للتأمل والتدبير فى أمر الله (جل وعلا) بالعلم والتفقه فى الأمر فى قوله تعالى:

---

(١) ألفن توفلر – مرجع سابق – ص ٢٤.

﴿ وَهُوَ الَّذِي جَعَلَ لَكُمُ النُّجُومَ لِتَهْتَدُوا بِهَا فِي ظُلُمَاتِ الْبَرِّ وَالْبَحْرِ قَدْ فَصَّلْنَا الآيَاتِ لِقَوْمٍ يَعْلَمُونَ (٩٧) وَهُوَ الَّذِي أَنشَأَكُم مِّن نَّفْسٍ وَاحِدَةٍ فَمُسْتَقَرٌّ وَمُسْتَوْدَعٌ قَدْ فَصَّلْنَا الآيَاتِ لِقَوْمٍ يَفْقَهُونَ (٩٨) ﴾(١).

وللتفكر فى خلق الله وما أنبت من زرع والتعقل فى ما سخره الله جل وعلا من الليل والنهار والشمس والقمر، قال تعالى:

﴿ يُنبِتُ لَكُم بِهِ الزَّرْعَ وَالزَّيْتُونَ وَالنَّخِيلَ وَالأَعْنَابَ وَمِن كُلِّ الثَّمَرَاتِ إِنَّ فِي ذَلِكَ لآيَةً لِّقَوْمٍ يَتَفَكَّرُونَ (١١) وَسَخَّرَ لَكُمُ اللَّيْلَ وَالنَّهَارَ وَالشَّمْسَ وَالْقَمَرَ وَالنُّجُومُ مُسَخَّرَاتٌ بِأَمْرِهِ إِنَّ فِي ذَلِكَ لآيَاتٍ لِّقَوْمٍ يَعْقِلُونَ (١٢) ﴾(٢).

وفى التفكر فى قدرة الله – جل وعلا – على الحياة والموت لأبلغ معنى لإعمال العقل، يقول تعالى: ﴿ وَهُوَ الَّذِي يُحْيِي وَيُمِيتُ وَلَهُ اخْتِلافُ اللَّيْلِ وَالنَّهَارِ أَفَلا تَعْقِلُونَ ﴾(٣).

لقد أمر الله جل وعلا بنى الإنسان بالعمل والمعرفة، والتدبر فى الأمر والتفكر فى الخلق، وذلك للمنفعة ولصالح البشرية، فما كان من الإنسان إلا أنه طغى واستكبر، وظن أنه بما وصل إليه من علم وما اخترعه من تقنيات وتكنولوجيا، قادر على أمر الكون، ولكن الأمر كله بيد الله – جل وعلا –: ﴿ غَافِرِ الذَّنبِ وَقَابِلِ التَّوْبِ شَدِيدِ الْعِقَابِ ذِي الطَّوْلِ لا إِلَهَ إِلاَّ هُوَ إِلَيْهِ الْمَصِيرُ ﴾(٤).

و: ﴿ الَّذِي بِيَدِهِ الْمُلْكُ وَهُوَ عَلَىٰ كُلِّ شَيْءٍ قَدِيرٌ ﴾(٥).

---

(١) سورة الأنعام الأيات: ٩٧، ٩٨.
(٢) سورة النحل – الآيات: ١١، ١٢.
(٣) سورة المؤمنون – الآية: ٨٠.
(٤) سورة غافر – الآية: ٣.
(٥) سورة الملك – الآية: ١.

فمن الأهمية أن يتدخل المُشرع لمواجهة هذا المد الجارف، الذى حمل لمجتمعنا مسالب العلم ومساوئ التكنولوجيا، فإن كان الأمر يحمل جوانب مفيدة، إلا أنه كذلك له جوانب ضارة بالمجتمع ومهدده لمستقبل أبناءه.

﴿ذلك فضل الله يؤتيه من شاء والله ذو الفضل العظيم﴾ .

# المراجع

# (المراجــع)(*)

**أولاً: الكتب القانونية:**


**• د/ إبراهيم حامد طنطاوي.**

- سلطات مأمور الضبط القضائي – المكتبة القانونية – القاهرة ط ٢ – سنة ١٩٩٧.

**• د/ أحمد حسام طه.**

- الجرائم الناشئة عن استخدام الحاسب الآلي – القاهرة – دار النهضة العربية – ط أولى – سنة ٢٠٠٠.

**• د/ أحمد ضياء الدين خليل.**

- مشروعية الدليل في المواد الجنائية – بدون ناشر – سنة ١٩٨٣.

**• أ/ أحمد عثمان حمزاوي.**

- موسوعة التعليقات على قانون الإجراءات الجنائية – دار النشر للجامعات المصرية – القاهرة – سنة ١٩٥٣.

**• د/ أحمد فتحي سرور.**

- الوسيط في قانون العقوبات (القسم الخاص) – دار النهضة العربية – سنة ١٩٩١.
- الوسيط في قانون العقوبات (القسم العام) – دار النهضة العربية – سنة ١٩٨٥.
- الشرعية الدستورية وحقوق الإنسان في الإجراءات الجنائية – دار النهضة العربية – ١٩٩٣.
- الوسيط في قانون الإجراءات الجنائية – دار النهضة العربية – ط ٤ – سنة ١٩٨١، وط ٧ – سنة ١٩٩٧.


---

(*) تم أثبات المراجع التى تم الاستعانه بها فى الدراسة بشكل أساسى، وبالنسبة للمراجع التى تم الاستعانه بها فى مواضع معينة، اكتفى بذكرها فى هذه المواضع.

• د/ إيهاب فوزي السقا.
- الحماية الجنائية والأمنية لبطاقات الأئتمان – دار الجامعة الجديدة – سنة ٢٠٠٧.
• د/ توفيق الشناوي.
- فقه الإجراءات الجنائية – دار الكتاب العربي – القاهرة – ط ٢ – سنة ١٩٥٤.
• د/ جميل عبد الباقي الصغير.
- الإنترنت والقانون الجنائى (الأحكام الموضوعية للجرائم المتعلقة بالإنترنت) – دار النهضة العربية – القاهرة – ط أولى – سنة ٢٠٠١.
- القانون الجنائى والتكنولوجيا الحديثة (الجرائم الناشئة عن استخدام الحاسب) – دار النهضة العربية – القاهرة – ط أولى – سنة ١٩٩٢.
- أدلة الإثبات الجنائى والتكنولوجيا الحديثة – دار النهضة العربية – سنة ٢٠٠١.
• د/ حسام محمود لطفي.
- الحماية القانونية لبرامج الحاسب الاليكترونى – دار الثقافة للطباعة والنشر – القاهرة – سنة ١٩٨٧.
• د/ رءوف عبيد.
- أصول علمى الإجرام والعقاب – دار الفكر العربى – القاهرة – ط ٥ – سنة ١٩٨١.
- مبادئ الإجراءات الجنائية (فى القانون المصرى) – دار الفكر العربى – سنة ١٩٨٢.
- المشكلات العملية الهامة فى الإجراءات الجنائية – دار الفكر العربى – جـ١ – ط ٣– سنة ١٩٨٠.

• د/ رمسيس بهنام.
- النظرية العامة للقانون الجنائى - منشأة المعارف - الإسكندرية - سنة ١٩٩٥.
- الإجراءات الجنائية (تأصيلا وتحليلا) - منشأة المعارف - سنة ١٩٨٤.
• د/ سامي حسني الحسيني.
- النظرية العامة للتفتيش فى القانون المصرى والمقارن - دار النهضة - سنة ١٩٧٢.
• د/ سليمان عبد المنعم.
- النظرية العامة لقانون العقوبات - دار الجامعة الجديدة - سنة ٢٠٠٠.
- بطلان الإجراء الجنائى - دار الجامعة الجديدة - سنة ٢٠٠٨.
• د/ عبد الرءوف مهدي.
- شرح القواعد العامة للإجراءات الجنائية - دار النهضة العربية - القاهرة - ٢٠٠٢.
• د/ عبد الفتاح بيومي حجازي.
- مبادئ الإجراءات الجنائية (فى جرائم الكمبيوتر والإنترنت) - دار الفكر الجامعى - الإسكندرية - ط أولى - سنة ٢٠٠٦.
- الأحداث والإنترنت - دار الفكر الجامعى - سنة ٢٠٠٤.
• د/ علي عبد القادر القهوجي.
- الحماية الجنائية لبرامج الحاسب - دار الجامعة الجديدة - سنة ١٩٩٧.
- علم الإجرام وعلم العقاب - الدار الجامعية - بيروت - سنة ١٩٩٠.
• د/ عمر محمد أبو بكر بن يونس.
- الجرائم الناشئة عن استخدام الإنترنت - دار النهضة العربية - القاهرة - سنة ٢٠٠٤.

- الاتفاقية الأوروبية للجريمة الافتراضية – طبعة أولى مصرية – بدون ناشر – سنة ٢٠٠٥ .

• د/ عوض محمد عوض.

- المبادئ العامة في قانون الإجراءات الجنائية – دار المطبوعات الجامعية – الإسكندرية – سنة ١٩٩٩ ، وطبعة منشأة المعارف – سنة ٢٠٠٢ .

• لواء د/ قدري عبد الفتاح الشهاوي.

- مناط التحريات (الاستدلال والاستخبارات) – منشأة المعارف – الإسكندرية – سنة ١٩٩٨ .

• محمد المرقي.

- الشرطة في مواجهة الجريمة – دار القاهرة للطباعة والنشر – القاهرة – سنة ١٩٧٧ .

• محمد أمين أحمد الشوابكة.

- جرائم الحاسب والإنترنت (الجريمة المعلوماتية) – مكتبة دار الثقافة للنشر والتوزيع – عمان – ط أولى – سنة ٢٠٠٤ .

• د/ محمد أنس جعفر.

- الوسيط في القانون العام – دار النهضة العربية – ط ٢ – سنة ١٩٩٠ .

• د/ محمد حسام لطفي.

- الحماية القانونية لبرامج الحاسب الآلي – دار الثقافة للطباعة والنشر – القاهرة – سنة ١٩٨٧ .

• د/ محمد زكي أبو عامر.

- الأثبات في المواد الجنائية – الفنية للطباعة والنشر – الإسكندرية – بدون سنة نشر .

- الإجراءات الجنائية – دار المطبوعات الجامعية – الإسكندرية – سنة ١٩٨٤ .

• محمد محمد شتا.

- فكرة الحماية الجنائية لبرامج الحاسب الآلى - دار الجامعة الجديدة - سنة ٢٠٠١.

• د/ محمود نجيب حسني.

- شرح قانون العقوبات (القسم العام) - دار النهضة العربية - سنة ١٩٨٨ .

• د/ نائلة عادل فريد قورة.

- جرائم الحاسب الاقتصادية (دراسة نظرية تطبيقية) - منشورات الحلبى القانونية - القاهرة - سنة ٢٠٠٥ .

• نبيلة هبة هروال.

- الجوانب الإجرائية لجرائم الإنترنت (فى مرحلة جمع الاستدلالات) دار الفكر الجامعى - الإسكندرية - سنة ٢٠٠٦ .

• لواء/ نجاح محمد فوزي.

- وعى المواطن العربى تجاه جرائم الاحتيال (بطاقات الدفع الإلكترونى) - الرياض - جامعة نايف للعلوم الأمنية - سنة ١٤٢٨هـ - ٢٠٠٧م.

• د/ هدي حامد قشقوش.

- جرائم الحاسب الآلى فى التشريع المقارن - دار النهضة العربية - سنة ١٩٩٢.

• د/ هشام محمد فريد رستم.

- قانون العقوبات ومخاطر تقنية المعلومات - مكتبة الآلات الحديثة - أسيوط - سنة ١٩٩٤ .

- الجوانب الإجرائية للجرائم المعلوماتية (دراسة مقارنة) - مكتبة الآلات الحديثة - أسيوط - سنة ١٩٩٤.

● د/ هلالي عبد اللاه أحمد.
- حجية المخرجات الكمبيوترية فى المواد الجنائية - دار النهضة العربية - ١٩٨٨.
- شرح قانون العقوبات (القسم العام) - دار النهضة العربية - ط أولى - ١٩٨٧.
- قانون العقوبات وأزمة الحاسبات - دار النهضة العربية - سنة ١٩٩٨م.
- الجوانب الموضوعية والإجرائية لجرائم المعلوماتية (على ضوء اتفاقية بودابست ٢٠٠١) - دار النهضة العربية - سنة ٢٠٠١.
- تفتيش نظم الحاسب الآلى، وضمانات المتهم المعلوماتى (دراسة مقارنة) - دار النهضة العربية - القاهرة - سنة ٢٠٠٠.
- المركز القانونى للمتهم فى مرحلة التحقيق الإبتدائى (دراسة مقارنة) - دار النهضة العربية - ط ٢ - سنة ٢٠٠٤.

ثانياً: الكتب العامة:

● د/ إبراهيم عبد الهادي المليجي وآخر.
- العولمة وأثرها فى التخطيط الاجتماعى - المكتب الجامعى الحديث - الاسكندرية - سنة ٢٠٠٥.

● لواء د/ بهاء الدين ابراهيم محمود.
- الشرطة والأمن الداخلى (فى مصر القديمة) - طبع ونشر هيئة الآثار المصرية - وزارة الثقافة - القاهرة - سنة ١٩٨٦.

● د/ سامي شلبي.
- مواجهة أزمة الكمبيوتر عام ٢٠٠٠ فى الواقع العربى (إخماد عاصفة القرن) - الشركة العربية للإعلام العربى - القاهرة - ط أولى - سنة ١٩٩٨.

● د/ عبد الحليم شوشه.

– الإلكترونيات وتطبيقاتها فى الاتصالات والحاسبات والتحكم – مركز الأهرام للترجمة والنشر – القاهرة – سنة ٢٠٠٢ .

● د/ علي القاسمي.

– مقدمة فى علم المصطلح – مكتبة النهضة المصرية – القاهرة – ط ٢ – سنة ١٩٩٧ .

● د/ علي يوسف علي.

– معجم مصطلحات الحاسب – دار خوارزم – القاهرة – سنة ١٩٩٩ .

● د/ طارق إبراهيم الدسوقي عطيه.

– الشخصية الإنسانية (بين الحقيقة وعلم النفس) – دار الجامعة الجديدة – الاسكندرية – ٢٠٠٧ .

● لواء د/ عصمت عدلي.

– علم الاجتماع الآمنى (الأمن والمجتمع) – دار المعرفة الجامعية – الإسكندرية – سنة ٢٠٠٣ .

● د/ محمد أحمد فكيرين.

– أساسات الحاسب الآلى – الراتب الجامعى – بيروت – لبنان – سنة ١٩٩٣ .

● د/ محمد فهمي طلبة وآخرون.

– الحاسب والذكاء الاصطناعى – موسوعة دلتا كمبيوتر – مطابع المكتب المصرى الحديث – القاهرة – سنة ١٩٩٤ .

– الموسوعة الشاملة لمصطلحات الحاسب الاليكترونى – موسوعة دلتا كمبيوتر ٢ – سنة ١٩٩١ .

– فيروسات الحاسب وأمن البيانات – موسوعة دلتا كمبيوتر – مطابع المكتب المصرى الحديث – سنة ١٩٩٢ .

- د/ محمد تيمور عبد الحسيب، د/ محمود علم الدين.

– الحاسبات الاليكترونية وتكنولوجيا الأتصال – دار الشروق – ط أولى – سنة ١٩٩٧ .

- د/ محمد محمد الهادي.

– تكنولوجيا المعلومات وتطبيقها – دار الشروق – القاهرة – ط أولى – سنة ١٩٨٩.

**ثالثاً: الرسائل العلمية:**

- د/ أيمن عبد الله فكري.

– جرائم نظم المعلومات – رسالة دكتوراه – كلية الحقوق – جامعة المنصورة – سنة ٢٠٠٥.

- د/ خالد حمدي عبد الرحمن.

– الحماية القانونية للكيانات المنطقية – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس – سنة ١٩٩٢ .

- راشد عايض المري.

– مدى حجية الوسائل التكنولوجية الحديثة فى إثبات العقود التجارية – رسالة دكتوراه – كلية الحقوق – جامعة القاهرة – سنة ١٩٩٨ .

- عزة محمود أحمد خليل.

– مشكلات المسئولية المدنية فى مواجهة فيروس الحاسب الآلى (دراسة مقارنة) – رسالة دكتوراه – كلية الحقوق – جامعة القاهرة – سنة ١٩٩٤.

- عمر محمد أبو بكر بن يونس.

– الجرائم الناشئة عن استخدام الانترنت (الأحكام الموضوعية والجوانب الإجرائية) – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس – سنة ٢٠٠٤.

• مرفت محمد البارودي.

– المسئولية الجنائية للإستخدامات السلمية للطاقة النووية – رسالة دكتوراه – كلية الحقوق – جامعة عين شمس – سنة ١٩٩٣.

رابعاً: الأبحاث والمقالات:

• أيمن عبد ا لحافظ.

– المخاطر التى تتعرض لها شبكة الإنترنت وسبل حمايتها – مجلة بحوث الشرطة – القاهرة – العدد ٢٢ – يوليو ٢٠٠٢.

• أ/ جمال محمد غيطاس.

– التعديلات الدستورية ... وحق الحصول على المعلومات – جريدة الأهرام – العدد ٤٣٩٠٥ – ٢٠ فبراير ٢٠٠٧.

• أ/ حسن مظفر الرزو.

– الأمن المعلوماتى (معالجة قانونية أولية) – مجلة الأمن والقانون – أكاديمية الشرطة – دبى – السنة ١٢ – العدد الأول – يناير ٢٠٠٤.

• لواء/ عادل عبد العليم.

– علم المصطلح الأمنى الجديد بعد أحداث ١١ سبتمبر – مجلة مركز بحوث الشرطة – أكاديمية مبارك للأمن – القاهرة – العدد ٢٢ يوليو ٢٠٠٢.

• د/ علي عبد القادر القهوجي.

– الحماية الجنائية لبرامج الحاسب الآلى – مجلة الحقوق للبحوث القانونية – كلية الحقوق – جامعة الإسكندرية – سنة ١٩٩٢.

• د/ عمر الفاروق الحسيني.

– تأملات فى بعض صور الحماية الجنائية لبرامج الحاسب – مجلة المحامى – الكويت – س ١٢ – نوفمبر / ديسمبر ١٩٨٩.

• د/ غنام محمد غنام.

– عدم ملائمة القواعد التقليدية فى قانون العقوبات لمكافحة الكمبيوتر –

مؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون – جامعة الإمارات – مايو ٢٠٠٠ .

● د/ محمود محمد عبد النبي.

– جرائم الحاسب الآلى – (الجزء الأول) – مجلة الأمن العام – العدد ١٨٨ – يناير ٢٠٠٥ .

– جرائم الحاسب الآلى – (الجزء الثانى) – مجلة الأمن العام – العدد ١٨٩ – أبريل ٢٠٠٥ .

● لواء د/ محمود وهيب السيد.

– مفاهيم أساسية فى أمن المعلومات – مجلة الأمن العام – القاهرة – العدد ١٨٣ – أكتوبر ٢٠٠٣ .

● د/ هشام محمد فريد رستم.

– جرائم الحاسب كصورة من صور الجرائم الاقتصادية المستحدثة – بحث مقدم إلى مجلة الدراسات القانونية – جامعة أسيوط – العدد ١٧ سنة ١٩٩٥ .

– أصول التحقيق الجنائى والفنى – مؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات – سنة ٢٠٠٠ .

● د/ هلالي عبد اللاه أحمد.

– حجية المخرجات الكمبيوترية – مؤتمر القانون والكمبيوتر والإنترنت – جامعة الإمارات – سنة ٢٠٠٠ .

**خامساً: المؤتمرات:**

● المؤتمر الأول لوزراء الداخلية العرب – القاهرة – سبتمبر ١٩٧٧ .

● مؤتمر إدارة أزمة الحاسبات – مركز شبكة المعلومات – جامعة أسيوط – سنة ١٩٩٨ .

- مؤتمر القانون والكمبيوتر والإنترنت – كلية الشريعة والقانون – جامعة الإمارات – دولة الإمارات – مايو ٢٠٠٠.
- المؤتمر السادس للجرائم المعلوماتية – أكاديمية الشرطة – القاهرة – من ١٣–١٥ أبريل ٢٠٠٥.
- المؤتمر الدولى الخامس عشر للجمعية الدولية لقانون العقوبات – ريو دى جانيرو – البرازيل – ٤ : ٩ سبتمبر ١٩٩٤.

- اللغة الفرنسية:

* ANTONIU (Georgo): "Les crimes informatiques et d'Autres crimes Dans le domaine de la Technologie informatique en Roumanie" R.I.D.P. 1993, p. 551.

* B. Bergnans, Le Vol d'information en droit comparé, R.D.P.C., 1988, No 8-9-10, p. 905.

* D. B. Parker: Comibattre La criminalité informatique, édoros 1987,p.18.

* FRANCILLON (jacques): "Les crimes informatiques et d'autres crimes dans le domaine de la technologie informatique en France" R.I.D.P. 1993, p. 309.

* GROZE (H.): "L'Apport du Droit Pénal a'la théorie générale du droit de L'informatique", J.C.P. 1988, 333, No. 16.

* Jaeger (Mare): "Les crimes informatiques et d'autres crimes dans le domaine le de la Technologic informatique au Lutembourg", R.I.D.P. 1993, p. 467.

* JEANDIDIER (Wilfrid): "droit Pénal Général", Montchrestien, Paris, 1988, N°. 16, p. 225.

* KEBEICH (M.): "L'inculpation, étude du droit francais, essai de ropprochement avecde droit egyption et Le droit des Etats-unis D'Amerique: thése Poitiers, 1984.

* Klaus Tedeman, Fraude et eutres délits d'affaires commis a L'aide d'ordinatewres électroniques, Rev. D.P.C. 1984, No. 7, p. 612.

* K. Trédmann,: Fraude et autres délits d'affaires connis a l'aide d'ordinateurs électroniques, Rev, drpén. crim, 1984, p. 612.

* Le primcipe de la legalité de la reuve penale.

* MERLE (R.): "L'incalpation in problemés contemparains de procédure Pénale: Mélanges HUGUENEY, Sirey, Paris, 1964.

* Michel vivant, commerçe élétronique cherche droit, droit, droit et patrimoine, No, 55, Décembre 1991, p. 50.

* M. Masse: La droit penal special né de I'informatique in ibformatique et droit pénal travaux de I'institut de sciences criminelles de poictiers 1981 - 4 éd cujas. p. 23.

* Pradel, Conclusion du colloque Informatiique et droit pénal, Paris, cujas, 1983, p. 155.

- اللغة الإنجليزية:

* Durhan (Cole): "The Emerging structures of criminal information Law: Tracing the contours of a New Poradigm". R.I.D.P. 1993, p. 111.

* FERBRACHE (CAVID): "Pathology of Computer Visruses", Sprnger Verlay' London LTD. 1992. p. 233.

* Joseph E. Collins, States improve computer crime law with private sector input, Data Management, Juin 1987, p. 5.

* JUNIOR (João Marcello de Araujo): "Computer Crimes and other Crimes Against information Technology in Brazil" R.I.D.P. 1993, p. 198.
* KASPERSEN (W.K. Henrik): "Computer crimes and other erimes against information tech nology in the Netherlands" r.I.D.P. 1993. p. 479.
* KERTESZ (Imre) and PUSZTAI (Laszlo): Computer crimes and other Crimes against information Technology in Hungary. R.I.D.P. 1993, p. 387.
* KUNSEMULLER (Carlos): "Computer Crimes and Other Crimes. Against Information Technology in Chilé R.I.D.P. 1993, p. 358.
* MOHRENSCHLAGER (Manfred): "Computer crimes and other crimes against information technology in Germany" R.I.D.P. 1993, p. 351.
* PIHLAJAMAKI (Antti): "Computer crimes and other crimes against information technology in Finland. R.I.D.P. 1993. p. 286.
* Sieber ulrich: The international Emergence of criminal information Law, cral Heymanns verlag K.G., 1992, pp. 3-27.
* SIEBER (Ulrich): "Computer crimes and other crimes against information Technology" - Commentary and Preparatory questions for the colloquium of the A.I.D.P. in Wurzburg. R.I.D.P. 1993, p. 77.
* YAMAGUCHI (Atsushi): "Computer crimes and other crimes... in Japan" R.I.D.P. 1993, p. 448.

# (الفهرس)

| | |
|---|---|
| رقم الإيداع | ٢٠٠٨/١٠٦٧٩ |
| الترقيم الدولى | I.S.B.N |
| 977-328-473-5 | |

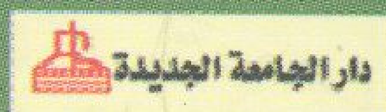
# الأمن المعلوماتى

## النظام القانونى للحماية المعلوماتية

Système judiciaire Pour
La Protection de L'informatique




دكتور
طارق إبراهيم الدسوقى عطية









٣٨-٤٠ ش سوتير - الأزاريطة - الأسكندرية

تليفاكس : ٤٨٦٨٠٩٩ - ٤٨٦٣٦٢٩-٤٨٥١١٤٣

E-mail: darelgamaaelgedida@hotmail.com